International Journal of Distributed Sensor Networks, 3: 243–272, 2007
Copyright © Taylor & Francis Group, LLC
ISSN: 1550-1329 print/1550-1477 online
DOI: 10.1080/15501320600781078

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

Redundancy Analysis and a Distributed Self-Organization Protocol for Fault-Tolerant Wireless Sensor Networks*

YI ZOU

Unitrends Software Corp., Columbia, SC, USA

KRISHNENDU CHAKRABARTY

Department of Electrical and Computer Engineering, Duke University, Durham, NC, USA

Sensor nodes in a distributed sensor network can fail due to a variety of reasons, e.g., harsh environmental conditions, sabotage, battery failure, and component wear-out. Since many wireless sensor networks are intended to operate in an unattended manner after deployment, failing nodes cannot be replaced or repaired during field operation. Therefore, by designing the network to be fault-tolerant, we can ensure that a wireless sensor network can perform its surveillance and tracking tasks even when some nodes in the network fail. In this paper, we describe a fault-tolerant self-organization scheme that designates a set of backup nodes to replace failed nodes and maintain a backbone for coverage and communication. The proposed scheme does not require a centralized server for monitoring node failures and for designating backup nodes to replace failed nodes. It operates in a fully distributed manner and it requires only localized communication. This scheme has been implemented on top of an energy-efficient self-organization technique for sensor networks. The proposed fault-tolerance-node selection procedure can tolerate a large number of node failures using only localized communication, without losing either sensing coverage or communication connectivity.

Keywords Connected Dominating Set; Fault Tolerance; Localized Communication; Network Organization; Sensor Networks; Topology Control

1. Introduction

Wireless sensor networks can be deployed to provide continuous surveillance and monitoring over a designated area of interest [2,7,19,22]. Many wireless sensor nodes have low cost and small form factors [1,2,7]; therefore, they can be deployed in large numbers with high redundancy. A typical example of such low-cost sensor nodes is the set of Berkeley

*A preliminary and abridged version of this paper was published in *Proc. IEEE DCOSS Conf. (Lecture Notes in Computer Science LCNS 3560)*, pp. 191–205, 2005. This research was supported by DARPA, and administered by the Army Research Office under Emergent Surveillance Plexus MURI Award No. DAAD19-01-1-0504. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the sponsoring agencies.

This work was carried out when Yi Zou was working as a post-doc research associate at the Department of Electrical and Computer Engineering, Duke University.

Address correspondence to Krishnendu Chakrabarty, Department of Electrical and Computer Engineering, Duke University, 129 Hudson Hall, Box 90291, Durham, NC 27708, USA, Tel.: 919-660-5244, Fax: 919-660-5293. E-mail: krish@ee.duke.edu

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Redundancy Analysis and a Distributed Self-Organization Protocol for Fault-Tolerant Wireless Sensor Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Duke University,Department of Electrical and Computer Engineering,Durham,NC,27708**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**30**	

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

motes from Crossbow Technology [33]. Since nodes are deployed in a redundant fashion, not every node in the network needs to be continuously active for sensing and communication. The operational lifetime of sensor networks can be increased by network organization schemes for topology control, where only a subset of nodes are kept active, while the other nodes are kept in a sleep state or a power-saving mode [14,27,31]. Fewer active nodes also place less demand on the limited network bandwidth.

Since a wireless sensor network should ideally perform surveillance tasks in an unattended manner, it needs to operate as long as possible, even when many sensor nodes fail. This motivates our work on fault-tolerant self-organization. Most recent work aims to provide fault tolerance in the deterministic deployment of sensor nodes [9,17,21,24]. Much less attention has been devoted to distributed protocols that can replace failing nodes in the network with spare nodes. Failing sensor nodes result in coverage loss and breakage in communication connectivity, hence there is a need for a distributed node replacement protocol and self-organization scheme that designates nodes as fault tolerance (spare) nodes. Such a scheme should be fully distributed such that it can be scalable for a large number of nodes. It should only require localized communication to select backup nodes for fault tolerance, and it should not rely on a centralized server to identify and replace faulty nodes.

This paper presents redundancy analysis and a distributed self-organization scheme that ensures communication connectivity and sensing coverage when nodes fail, either sequentially or simultaneously. We first present analytical results to characterize the extent of redundancy needed for fault tolerance. We then describe a distributed scheme that achieves fault tolerance by selecting fault tolerance nodes that can replace failing nodes. The proposed distributed approach uses only single-hop or restricted-hop neighborhood information to select fault tolerance nodes. We show that the proposed approach provides communication connectivity and sensing coverage even when up to Ω nodes fail, where Ω is a user-defined parameter.

The paper is organized as follows. In Section 2, we briefly describe related prior work. In Section 3, we present the background and assumptions used in this paper. Section 4 describes fault tolerance for communication connectivity. Section 5 addresses fault tolerance for sensing coverage. We present simulation results for the proposed distributed self-organization technique in Section 6. Section 7 concludes the paper and outlines directions for the future work.

2. Related Work

Energy-efficient self-organization in wireless sensor networks has received considerable attention in the literature [13,16,20,23,26,29]. Energy considerations have been used to find a set of (active) nodes that can form a backbone for the network. Selection of these backbone nodes can be achieved by heuristics described in [3,4,25,28] based on the concept of a connected dominating set, where the distributed algorithm proposed in [3] has the best message complexity. The selection of active nodes to guarantee both sensing coverage and communication connectivity has been studied in [14,27,31]. A recent approach distinguishes connectivity from sensing, and determines the configuration of the nodes with both communication connectivity and sensing coverage as considerations [27].

Fault-tolerance in distributed sensor networks has received relatively less attention [9,17,21,24]. Problems studied include the characterization of sensor fault modalities [17,24], faulttolerance in multiple-sensor fusion [21], and reliable information dissemination [9]. Recent work on fault-tolerance in wireless sensor networks can be categorized as being focused on fault detection [6,10,12] or fault-tolerant operations [15,30]. In [10], the

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

authors present various fault tolerance techniques at different levels, including the physical layer for communication, the hardware components of a sensor node, system software such as the embedded operating system, middleware, and application. In [12], the authors consider faults in node sensor measurements and develop a distributed Bayesian algorithm to detect and correct such faults. [6] also addresses a similar fault detection problem, and presents a crash identification mechanism. In [30], the authors show that a sensor network with n nodes is asymptotically connected if each node is directly connected to at least 5.1774 log n neighboring nodes. [15] shows that for a wireless sensor network with n nodes, the connectivity probability with up to k failing nodes is at least $e^{e^{\alpha}}$ when the transmission radius r satisfies $n\pi r^2 \geq \ln n + (2k - 1) \ln \ln n - 2\ln k! + 2\alpha$. Recently, in [11], a protocol has been proposed for event detection in sensor networks, which is able to handle both natural and malicious node failures in sensor networks. However, most prior work has not characterized the redundancy necessary for fault tolerance, and no distributed self-organization protocol has directly considered this issue.

3. Preliminaries

3.1. Assumptions

The discussion in this paper is based on the following assumptions:

1. The ad hoc sensor network is deployed with a sufficient number of nodes such that the network is connected. All sensor nodes have the same maximum communication range r_c and maximum sensing range r_s.
2. We represent the surveillance field by a 2D grid, whose dimension is given as $X \times Y$. Let $\mathcal{G} = \{g_1, g_2, \cdots, g_m\}$ be the set of all grid points, and $m = |\mathcal{G}| = XY$.
3. We use S to denote the set of n sensor nodes that have been placed in the sensor field, i.e., $|S| = n$. A node with id k is referred to as $s_k (s_k \in S, 1 \leq k \leq n)$. Let d_i^k be the distance between the grid point g_i and the sensor node s_k. In a graph model $G(V, E)$ for a set S of nodes, we use the vertex $v \in V$ in the graph model interchangeably with its corresponding node $s \in S$. The set of edges E denotes the connectivity between nodes.
4. We model sensing coverage using the probability p_i^k that a target at grid point g_i is detected by a node s_k:

$$p_i^k = \begin{cases} e^{-\alpha d_i^k}, & \text{if } d_i^k \leq r_s; \\ 0, & \text{otherwise,} \end{cases} \tag{1}$$

where α is a parameter representing the physical characteristics of the sensor. The model conveys the intuition that the closer a location is to the node, a higher signal-to-noise ratio is expected, resulting in a higher confidence level that a target at that location is detected. Areas beyond the maximum sensing range r_s are then considered to be too noisy for the sensor node to determine if there is a target. The sensing model is only used for coverage evaluation during active node selection; alternative sensing models can also be easily considered. Assume that S_i is the set of nodes that can detect grid point g_i; thus the detection probability for grid point g_i is evaluated by Equation (1) as

$$p_i(S_i) = 1 - \prod_{s_k \in S_i} (1 - p_i^k) \tag{2}$$

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

3.2. Coverage- and Connectivity-centric Selection of Active Nodes for Self-organization

In this paper, we focus on the fault tolerance problem in the topology control of ad hoc sensor networks. We assume that a network organization scheme is provided to the sensor network. Network organization can be achieved by using techniques described in [14,27,31], which select a subset of active nodes as a backbone for communication connectivity and/or sensing coverage. The failure of these active nodes can result in loss of connectivity and/or loss of sensing coverage. We use S_a (S_s) to denote the set of active (sleeping) nodes determined by such active nodes selection algorithms, and the following discussion assumes that S_a and S_s have already been determined. We consider the threshold p_{th} to be a parameter underlying a successful sensing coverage over the sensor field. The following conditions are implicitly satisfied: 1) $\forall g_i \in \mathcal{G}$ and $S_i \subseteq S_a$, $p_i(S_i \geq p_{th}$; 2) $\forall s_k \in S_a$ is connected.

In [31], we have shown that the problem of selecting a subset of nodes as a backbone for both sensing coverage and communication connectivity is $\mathcal{NP}$-complete. We have also presented the token-based coverage- and connectivity-centric active node selection (CCANS) protocol that achieves self-organization with a subset of active nodes, which are responsible for both the coverage and the connectivity. In this section, we first review the token-based CCANS protocol for energy-efficient self-organization. We then describe the problem of providing fault tolerance to active backbone nodes in the following sections. The proposed fault-tolerant self-organization technique is general, and it can also be used with other self-organization protocols. CCANS is used in this paper as a vehicle to evaluate the proposed method.

3.3. Token-based CCANS Protocol

There are three types of messages used in this protocol, namely HELLO, STATE, and UPDATE. These messages contain such fields as *tokenid* and *srcid* which enables the token to control the execution of the sensing coverage evaluation and connectivity checking. There are three possible states for all nodes, namely UNSET, SLEEP and ACTIVE. Initially, all nodes are in UNSET state with their *tokenid* = –1, i.e., no token has been given to them for the execution of the CCANS algorithm. There are two stages in the CCANS protocol, namely Stage 1 for node *sensing coverage evaluation*, followed by Stage 2 for node *state and connectivity checking*. The node with the assigned token is referred to as the *token node* and all other nodes either collect messages sent from the token node or perform no action. In Stage 1, the current token node evaluates the coverage within its sensing area versus the coverage within its sensing area contributed by its neighbors. It chooses the state ACTIVE if its sensing area is not fully covered by its neighbors, otherwise it chooses the state SLEEP. However, this state decision is not final until the connectivity checking and coverage re-evaluation are completed in Stage 2. One node is pre-selected as the start node by the base-station to initiate the execution of the CCANS algorithm for finding a subset of active nodes.

The token passing procedure is designed to reduce the execution time of the algorithm by expanding the global sensing coverage as much as possible [31]. Consider an arbitrarily chosen node s_k. s_k gets the token for execution of the CCANS algorithm when $id(s_k) = tokenid$. If $tokensrc(s_k) = -1$, then s_k sets $tokensrc(s_k) = srcid$; this is set only once. Therefore, every node knows its token source and is able to pass the token back to its token source when it completes CCANS Stage 2. If s_k is the start node, then initially $tokensrc(s_k) = id(s_k) \neq -1$. At the time when the token is passed back to s_k, if s_k has no UNSET neighbors, it executes Stage 2 of the distributed CCANS procedure to find its own final state

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

decision; then the distributed CCANS procedure terminates. As an example, Fig. 1(a) illustrates token passing for an example sensor network with four sensor nodes, s_1, s_2, s_3, and s_4, where s_1 is the start node. The steps in this example are as follows:

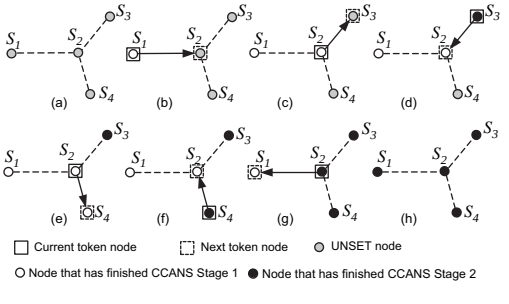
(a) Initially all nodes are in UNSET state and s_1 is the start node.
(b) s_1 has completed CCANS State 1 and passes the token to s_2.
(c) s_2 has completed CCANS Stage 1 and passes the token to s_3.
(d) s_3 has no more UNSET neighbors and it has completed CCANS Stage 2, therefore s_3 passes the token back to s_2.
(e) s_2 still has UNSET neighbors so s_2 passes the token to s_4.
(f) s_4 has no more UNSET neighbors and it has completed CCANS Stage 2, therefore s_4 passes the token back to s_2.
(g) s_2 has no more UNSET neighbors and it has completed CCANS Stage 2, therefore s_2 passes the token back to s_1.
(h) s_1 has no more UNSET neighbors and it has completed CCANS Stage 2. Since s_1 is the start node, all nodes have made the state decision, and CCANS terminates.

Fig. 1(b) shows the sequence of the token source in terms of node id during the execution of the distributed CCANS procedure for the example shown in Fig. 1(a). The CCANS procedure requires only constant rounds for message exchange in both stages [31]. Let Δ be the maximum node degree in the graph corresponding to the sensor network. The connectivity checking procedure in CCANS has a time complexity of $O(\Delta^2)$ per node, and this is carried out independently by each node. Since the sensing coverage evaluation is carried out per grid point for all nodes in the neighborhood, the time complexity of the sensing coverage evaluation in CCANS is $O(m\Delta)$, where m is the number of grid points representing the sensor field. Therefore, the overall time complexity for the CCANS procedure per node is $O(m\Delta + \Delta^2)$. The complexity depends only on the maximum degree of a node and the grid granularity of the sensor field. As shown in [31], the CCANS protocol always terminates and achieves self-organization. The completion of the distributed CCANS procedure can be easily notified to the base station.

3.4. Fault-tolerant Self-organization

In this paper, we focus on fault-tolerant self-organization, where both the sensing coverage and the connectivity are preserved with support from the designated fault tolerance (FT) nodes when active nodes fail. We refer to this as the fault-tolerance-nodes-selection

(a)



(b)

Step	Token Passing Sequence in Terms of Node Id
a	CCANS starts with s_1 as the start node.
b	$1 \rightarrow 2$
c	$1 \rightarrow 2 \rightarrow 3$
d	$1 \rightarrow 2 \rightarrow 3 \rightarrow 2$
e	$1 \rightarrow 2 \rightarrow 3 \rightarrow 2 \rightarrow 4$
f	$1 \rightarrow 2 \rightarrow 3 \rightarrow 2 \rightarrow 4 \rightarrow 2$
g	$1 \rightarrow 2 \rightarrow 3 \rightarrow 2 \rightarrow 4 \rightarrow 2 \rightarrow 1$
h	CCANS terminates.

FIGURE 1 (a) Example of token passing in the distributed CCANS procedure. (b) Token passing sequence for the example in Fig. 1(a).

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

(FTNS) problem. The proposed distributed FTNS algorithm is executed after S_a and S_s are determined, where a set S_t of nodes is designated to be FT nodes (backup nodes for active nodes). These FT nodes provide fault tolerance for the existing active nodes. They need not be active unless the active nodes that they are supporting fail. They can run in a power-saving mode and periodically query whether the active nodes are still alive using very limited bandwidth.

Note that simultaneous failures of nodes in S_a and S_t may result in loss in sensing coverage or breakage in communication connectivity since FT nodes are not backed up by nodes in S_t. However, if only FT nodes fail or FT nodes and their non-neighboring active nodes fail, the sensing coverage and communication connectivity are still guaranteed. Furthermore, the proposed distributed algorithm can be applied in a repeated manner to select more FT nodes for the previously selected FT nodes.

We assume that the number of nodes initially deployed in the sensor field is sufficient to achieve fault-tolerant operations, i.e., we have enough sleeping nodes available to select as FT nodes. Some observations and additional definitions are listed below:

- It is trivial to see that if all failing nodes are sleeping nodes, the existing active nodes can tolerate the failure of up to $|S_s|$ nodes.
- We define the maximum number of active nodes that can fail simultaneously without losing sensing coverage or communication connectivity as the *degree of fault tolerance (DOFT)*, denoted by Ω ($\Omega \geq 1$).
- The nodes that are selected from the set of sleeping nodes to obtain a Ω-DOFT wireless sensor network are referred to as Ω-fault-tolerant (Ω-FT) nodes. We denote the set of Ω-FT nodes as S_t^{Ω}.
- Let $S_t^0 = \phi$ and $S_a^{\Omega} = S_t^{\Omega} \cup S_a$. It follows that S_a^{Ω} provides a solution to the Ωj-DOFT FTNS problem. In other words, a Ω-DOFT FTNS-derived sensor network is still connected and provides undiminished coverage of the surveillance area if any Ω active nodes fail.

4. Connectivity-Oriented Fault Tolerance

In this section, we focus on the analysis of fault tolerance for communication connectivity. The discussion of fault tolerance for sensing coverage is presented in next section.

4.1. An Upper Bound on the Number of Fault Tolerance Nodes

We first consider the case of 1-DOFT, i.e., $\Omega = 1$. Let N_k be the set of neighbors for s_k, N_k^a be the set of active neighbors, and N_k^s be the set of sleeping neighbors. Let Δ_k be the number of neighboring nodes for s_k, Δ_k^a be the number of active neighboring nodes for s_k, and Δ_k^s be the number of sleeping neighboring nodes for s_k. In other words, $\Delta_k = |N_k|, \Delta_k^a = |N_k^a|$ and $\Delta_k^s = |N_k^s|$. It is trivial to see that $\forall s_k \in S$, $\Delta_k \geq 1$ otherwise S is not connected. Thus communication connectivity is not affected if any node in S_s fails. This is also true if multiple nodes in S_s fail. Therefore, any number of sleeping nodes in S_s can fail either sequentially or simultaneously. This implies that only active nodes need to be considered as failing nodes for the analysis of connectivity fault tolerance.

It can be seen that, if $\exists s_k \in S$ such that $\Delta_k = 1$, then Ω-DOFT ($\Omega \geq 1$) cannot be achieved for the network since when this neighbor node of s_k fails, s_k is disconnected from the rest of the network [32]. For any wireless sensor network with S_a ($S_a \neq \phi$), $\forall s_k \in S$, s_k is connected to at least one node in S_a, i.e., $\Delta_k^a \geq 1$. Therefore, $\Delta_k \geq \Delta_k^a \geq 1$. In a sensor network with S_a as a backbone for both sensing and communication, if $s_k \notin S_a$, i.e., s_k is a

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

sleeping node, we can expect $\Delta_k > 1$ due to the need for sensing coverage; otherwise an active node must be located expect at the same location as s_k. This observation leads to a lower bound on the node density required in the sensor field for fault tolerance. This lower bound can be used as a necessary condition for the fault-tolerant sensor node deployment.

Consider a total of n nodes with communication radius as r_c each in a sensor field with area A. In order to achieve Ω-DOFT ($\Omega \geq 1$), a lower bound on the total number of nodes n in the sensor field is given by: $n \geq \frac{3A}{\pi r_c^2}$. The proof, which can be found in [32], is straightforward and is therefore omitted. For example, consider the extreme case of $A = \pi r_c^2$. For this case, we must have $n \geq 3$. This is obviously true since if there are only two nodes, neither of them can fail. In the following discussion, we assume that the initial sensor deployment has provided a sufficient number of nodes for fault tolerance. Our goal is to designate extra sleeping nodes as back-up nodes, i.e., FT nodes, to provide fault tolerance when currently-selected active nodes fail. We also need to minimize the number of FT nodes. Before we present bounds on the number of FT nodes needed to achieve Ω-DOFT, we prove the following theorem.

Theorem 1. Let $s_k \in S$ be a node in the sensor network. Let the region that lies within the communication range r_c of s_k be A_k and let S* be the set of nodes within A_k*. Assume that all nodes in S* are connected to each other, i.e., $\forall s_i, s_j \in S$, there exists a routing path from s_i to s_j. In order to ensure communication connectivity between the nodes in S* if s_k fails, it is sufficient to have 10 nodes (not counting s_k) in A_k*.*

Proof. Let $G(V, E)$ be the connected graph representing S^*, i.e., $|V| = |S^*|$, v_k is the vertex representing $s_k \in S$, and $\forall u, v \in V$, $(u, v) \in E$ if $d(u, v) \leq r_c$. Let $G_c(V_c, E_c)$ be a subgraph corresponding to a connected-dominating-set (CDS) of G [3, 4, 8, 25, 28]. We first derive an upper bound on the number of vertices needed for a CDS. The circular area A_k* with radius r_c can be divided into six sectors, denoted by $A_1, \ldots, A_6$ in Fig. 2(a). Each sector A_i ($1 \leq i \leq 6$) has an opening angle of $\frac{\pi}{3}$. From Fig. 2(a), the nodes in S^* can be located in one or multiple sectors, corresponding to the vertices in V in these sectors. Excluding equivalent cases due to symmetry, we list all possibilities for the locations of the vertices in Fig. 2(b).

Case 1: All vertices are located in the same sector. Assume this sector is A_1 as shown in Fig. 2(b)[a]. Obviously, for any two vertices $\forall u, v \in V$ within A_1, $d(u, v) \leq r_c$, which includes the case where u and v can be located at the sector boundaries. We can simply let $V_c = \{u\}$ where u is an arbitrary chosen vertex. Therefore, $|V_c| = 1$. For example, if an active node s_k has only two neighbors in one sector, where there are a total 3 nodes within the communication region of s_k. Fault tolerance can be achieved for the failure of s_k because one of its two neighbors can be designated as a FT node.

Case 2: All vertices are located within two sectors. There are three possibilities for the sectors A_1 and A_2, as shown in Fig. 2(b)[b], 2(b)[c], and 2(b)[d], respectively. Since G is connected, $\exists (u, v) \in E$ such that u is in A_1 and v is in A_2. Moreover, $\forall u_i \in A_1$, $\exists (u, u_i) \in E$ and $\forall u_i \in A_2$, $\exists (u, u_i) \in E$. Therefore, $V_c = \{u, v\}$ is a CDS of G and $|V_c| \leq 2$.

Case 3: All vertices are located within three sectors. There are four possibilities for the sectors A_1, A_2, and A_3, as shown in Fig. 2(b)[e], 2(b)[f], 2(b)[g], and 2(b)[h], respectively. Let u be an arbitrarily-chosen vertex in A_1. Since G is connected, $\exists (u, v) \in E$

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

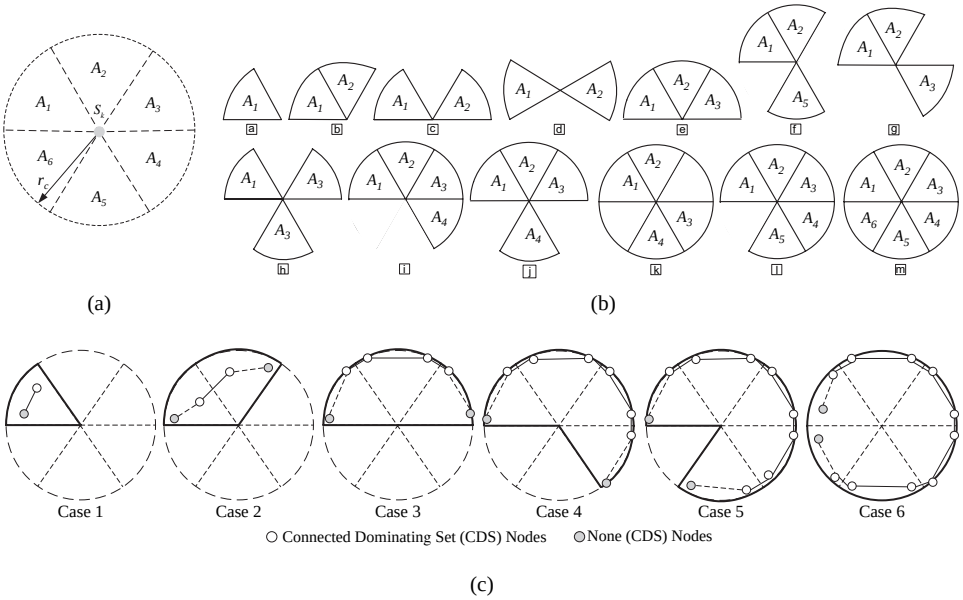


FIGURE 2 Illustration of the proof of Theorem 1: (a) A node's communication region can be divided into six sectors with an opening angle of $\frac{\pi}{3}$. (b) Proof of Theorem 1: All possibilities of vertices locations. (c) Illustration of the six cases corresponding to Theorem 1.

such that v is either in A_2 or in A_3. Without loss of generality, assume that v is in A_2. Similarly, for $w \in A_3$, $\exists(w, x) \in E$ such that x is either in A_1 or in A_2. Therefore, $V_c = \{u, v, w, x\}$ is a CDS of G and $|V_c| \leq 4$.

Case 4: All vertices are located within four sectors. There are three possibilities for the sectors A_1, A_2, A_3, and A_4 as shown in Fig. 2(b)i, 2(b)j, and 2(b)k, respectively. Divide these four sector areas into two groups where one group has three sectors and the other group has one sector. Assume that A_1, A_2 and A_3 are in one group the other group contains A_4. From Case 2, $\exists(u, v) \in E$, where u is in A_4 and v is in A_1, or A_2 or A_3. Furthermore, from the proof for Case 3, $\exists V_1 = \{w_1, w_2, w_3, w_4\}$, where V_1 is a CDS for vertices in A_1, A_2 and A_3. Therefore, $V_c = \{u, v, w_1, w_2, w_2, w_4\}$ is a CDS of G and $|V_c| \leq 6$.

Case 5: All vertices are located within five sectors. There is only one possibility for the sectors A_1, A_2, A_3, A_4, and A_5 as shown in Fig. 2(b)l. Similar to the proof for Case 4, we divide these five sector areas into two groups where one group contains any four of these five sectors and the other group contains the remaining sector. Assume that A_1, A_2, A_3, A_4 are in the one group and A_5 is in the other group. From Case 2, $\exists(u, v) \in E$, where u is in A_5 and v is in A_1, or A_2, or A_3, or A_4. Furthermore, from the proof for Case 4, $\exists V_1 = \{w_1, w_2, w_2, w_3, w_4, w_5, w_6\}$, where V_1 is a CDS for vertices in A_1, A_2, A_3 and A_4. Therefore, $V_c = \{u, v, w_1, w_2, w_2, w_3, w_4, w_5, w_6\}$ is a CDS of G and $|V_c| \leq 8$.

Case 6: Vertices are located in all six sectors. There is only one possibility for the sectors A_1, A_2, A_3, A_4, A_5, and A_6 as shown in Fig. 2(b)m. Similar to Case 3 and Case 4, we divide these six sectors into two group where one group contains five sector areas and the other group contains one sector area. Assume that A_1, A_2, A_3, A_4, A_5 are in the one group and A_6 is in the other group. From Case 2, $\exists(u, v) \in E$, where u is in A_6 and v is

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

in A_1, or A_2 or A_3 or A_4 or A_5. Furthermore, from Case 5, $\exists V_1 = \{w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8\}$, where V_1 is a CDS for vertices in A_1, A_2, A_3, A_4 and A_5. Therefore, $V_c = \{u, v, w_1, w_2, w_2, w_3, w_4, w_5, w_6, w_7, w_8\}$ is a CDS of G and $|V_c| \leq 10$.

The nodes corresponding to V_c thus keep all nodes in S^* connected even when s_k fails. Therefore, the maximum number of required FT nodes for s_k is 10.

Figure 2(c) illustrates each of the six cases discussed in Theorem 1. Based on Theorem 1, we can derive an upper bound on the number of FT nodes needed within the communication region of an arbitrarily-chosen node. Assume that N_k is the set of neighbor for $s_k \in S$. Consider the special case where $S = N_k \cup \{s_k\}$, i.e., all nodes in $S \backslash \{s_k\}$ are neighbors of s_k. Suppose the nodes in N_k are not connected. When s_k fails, $\exists s_i, s_j \in N_k$ such that no routing can be formed between s_i and s_j. Thus fault tolerance can only be achieved if there is sufficient node density in the network. Let Γ_k be the number of FT nodes required for an arbitrarily-chosen node s_k in a 1-DOFT sensor network. Next we present a sufficient condition relating fault tolerance with Γ_k in the following theorem.

Theorem 2. The network is 1-DOFT with respect to the failure of any node $s_k \in S_a$ if $\forall s_k \in S_a$, the nodes in N_k are connected and $\Gamma_k \geq 10$.

The proof of Theorem 2 is given in the appendix. Note that we need to have $\Gamma_k = 10$ only when s_k has no active neighbors, i.e., $\Delta_k^a = 0$. This is shown as Case 6 in Fig. 2(c). Since S_a as a backbone is a non-empty set that connects all nodes, $\Gamma_k = 10$ needs to be 10 only if $|S_a| = 1$ and $S_a = \{s_k\}$. This means that all nodes are deployed within s_k's communication region and only s_k is active. Generally, we have $\forall s_k \in S_a, |\Delta_k^a| \geq 1$ since $|S_a| > 1$, which implies the following corollary [32], which is proven in the appendix.

Corollary 1. When the number of active nodes is greater than one, i.e., $|S_a| > 1$, the sensor network is 1-DOFT with respect to the failure of any node $s_k \in S_a$ if $\forall s_k \in S_a$, N_k is connected and there are 9 or more FT neighboring nodes for s_k.

Corollary 1 shown that Δ_k^a is a measure of the communication connectivity support provided by the active neighbors of s_k when s_k fails. In fact $\Delta_k^a > 0$ implies that there exists built-in fault tolerance for s_k. The fault tolerance provided by the active neighbors in N_k^a decreases the maximum number of FT nodes needed when s_k fails. Note that the above is true only for $\Omega = 1$ since when $\Omega > 1$, nodes in N_k^a may also fail at the same time when s_k fails. Both Theorem 2 and Corollary 1 assume that when $s_k \in S_a$ fails, the selected FT nodes for s_k do not fail. Since FT nodes are selected to provide fault tolerance for active nodes in S_a, their own failures are not considered in the analysis. However, the same procedure of selecting FT nodes for active nodes in S_a can be applied repeatedly to select more FT nodes in a sequential manner.

Our goal in this paper is to develop is to develop a distributed self-organization algorithm, where nodes rely only on single-hop or restricted-hop knowledge. Therefore, we allow each active node $s_k \in S_a$ to select FT nodes only from its sleeping neighbors. Recall that we denote the set of FT nodes in a Ω-DOFT sensor network FT nodes as S_t^Ω. Let N_k^Ω be the set of FT neighbors for an arbitrarily-chosen $s_k \in S_a$ in a Ω-DOFT network. Obviously, $N_k^\Omega \subseteq N_k^s$ and $\Gamma_k = |N_k^\Omega|$. When each active node finds its corresponding N_k^Ω, the set S_t^Ω is determined, i.e., $S_t^\Omega = \bigcup_{\forall s_k \in S_a} N_k^\Omega$, where the total number of FT nodes in this Ω-DOFT sensor network is $|S_t^\Omega|$. Next, we derive an upper bound on the total number of FT nodes needed for the entire sensor network. Consider a wireless sensor network consisting of n nodes each with communication radius r_c. Let the set of nodes be denoted by S. Assume that all nodes in S are connected, i.e., $\forall s_i, s_j \in S$, there exists a routing path from s_i to s_j. Let $G(V,E)$ be the connected graph corresponding to S, i.e., $|V| = |S|$ and

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

v_k be the vertex representing $s_k \in S$, where $\forall u,v \in V$, $(u,v) \in E$ if $d(u,v) \le r_c$. Assume that S_a is the set of (active) backbone nodes. The subgraph corresponding to S_a is denoted by $G_a(V_a, E_a)$, where G_a is a CDS of G. Let S_t^1 be the set of nodes selected as FT nodes to achieve 1-DOFT. For 1-DOFT case, this bound is obtained directly from Theorem 3. The proof is given in the appendix.

Theorem 3. An upper bound on the total number of FT nodes needed to achieve 1-DOFT is given by:

$$|S_t^1| \le \begin{cases} 10, & \text{if } |V_a| = 1; \\ 9|V_a| - |E_a|, & \text{if } |V_a| > 1. \end{cases} \tag{3}$$

Next, we consider a more general fault tolerance scenario where $\Omega > 1$. Note that we assume $|S_a| \ge \Omega$ for the analysis of Ω-DOFT; otherwise Ω-DOFT is not meaningful. In the following, we determine the number of nodes Γ_k needed for an arbitrarily-chosen active node to achieve Ω-DOFT in its communication region. In the following, we assume that $\Delta_k^a \ge \Omega - 1$ to simplify the discussion. Note also that since $\Omega > 1$, we have $|S_a| > 1$. Therefore, we can ignore the special case where only one node is active and all other nodes are placed within its communication range.

Theorem 4. The network is Ω-DOFT ($\Omega > 1$) with respect to failures of any Ω nodes inside the communication region of an arbitrarily-chosen $s_k \in S_a (1 < \Omega \le \Delta_k^a + 1)$, if the nodes in N_k are connected and $\Gamma_k \ge \Omega$. Moreover, Γ_k is lower-bounded by the following:

$$\Gamma_k \ge \begin{cases} \Omega + 9, & \text{if } s_k \text{ fails and } \Omega = \Delta_k^a + 1; \\ \Omega + 8, & \text{if } s_k \text{ fails and } \Omega < \Delta_k^a + 1; \\ \Omega, & \text{if } s_k \text{ does not fail.} \end{cases} \tag{4}$$

The proof of Theorem 4 is given in the appendix. We now present bounds on the total number of FT nodes needed to achieve Ω-DOFT ($\Omega > 1$ and $|S_a| \ge \Omega > 1$). Note that for a Ω-DOFT sensor network, if $\exists s_k \in S_a$ such that $\Omega > \Delta_k^a$, the DOFT in the communication region of s_k is at most $\Delta_k^a + 1$. In this case, since the maximum number of failing nodes within the communication region of s_k is at most $\Delta_k^a + 1$, Ω-DOFT for s_k refers to the failure of up to $\Delta_k^a + 1$ nodes inside the communication region of s_k, and the failure of $\Omega - (\Delta_k^a + 1)$ nodes outside the communication region of s_k. Thus, when Ω-DOFT is achieved for the entire sensor network, fault tolerance with the maximum number of failing nodes in the communication region of s_k is automatically achieved. Let $S_f \subseteq S_a$ be the set that contains Ω failing active nodes, where the subgraph representing S_f is denoted by $G_f(V_f, E_f)$. Let S_t^Ω be the set of nodes selected as FT nodes to achieve Ω-DOFT in the sensor network. This bound is given by Theorem 5. The proof is given in the appendix.

Theorem 5. An upper bound on the total number of FT nodes needed to achieve Ω-DOFT is given as

$$|S_t^\Omega| \le \begin{cases} 10|V_a| - 4|E_a|, & \text{if } G_f \text{ is connected;} \\ 9|V_a|, & \text{if } G_f \text{ is not connected and } E_f = \phi; \\ 9|V_a| - 2, & \text{if } G_f \text{ is not connected and } E_f \ne \phi. \end{cases} \tag{5}$$

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

4.2. Lower Bound on the Number of Fault Tolerance Nodes

To reduce energy consumption, it is desirable to minimize the number of FT nodes needed, i.e., to minimize the size of S_t^{Ω}. In this section, we present a lower bound on the number of FT nodes needed to achieve the required Ω-DOFT (Ω ≥ 1) in wireless sensor networks. Let $N_k^f \subseteq N_k^a$ be the set of failing active neighbors of s_k, i.e., $S_f = \bigcup_{s_k \in S_a} N_k^f$. Let $N_k^{\Omega} \subseteq N_k^s$ be the set of FT nodes for s_k, i.e., $S_t^{\Omega} = \bigcup_{s_k \in S_a} N_k^{\Omega}$.

We know from previous subsections that $\forall s_k \in S_a$, FT nodes of s_k keep all neighbors nodes of s_k in N_k connected. This implies that the subgraph representing N_k^{Ω} is a CDS of the subgraph representing N_k. When Ω = 1, the minimization of $|S_t^{\Omega}|$ is equivalent to finding the MCDS for the subgraph representing N_k for each active node $s_k \in S_a$. However, since no failing active node has any failing active neighbors for Ω = 1, such an MCDS for s_k also contains existing active neighbors in N_k^a as existing dominating nodes. Let S_t^1 be the set of nodes selected as FT nodes to achieve 1-DOFT in the sensor network. It is then easy to see that a lower bound on the total number of FT nodes needed to achieve 1-DOFT, i.e., $|S_t^1|$, is given by:

$$|S_t^1| \geq \begin{cases} 1, & \text{if } |S_a| = 1; \\ 0, & \text{if } |S_a| > 1. \end{cases} \tag{6}$$

Note that the best case of $|S_t^1| = 0$ when $|S_a| > 1$ rarely happens in practice, because it requires that neighbors of any active node are also neighbors of at least another active node. This implies that all nodes are within a circle of radius τ_c. Since $|S_a| > 1$, this makes the other $|S_a| - 1$ nodes unnecessary. It is possible to have several such nodes but if $|S_a|$ is very large, there will be a significant energy overhead for these nodes. When Ω > 1, the analysis is more complicated because when an active node s_k fails, some active neighbors in N_k^a may also fail at the same time.

To simplify the discussion, we define function $\mathcal{M}$ as follows: $\bar{S}_a = \mathcal{M}(S, S_a)$, where

1. $S_a \subseteq \bar{S}_a$;
2. The subgraph representing $\bar{S}_a$ is a connected dominating set (CDS) of the graph representing S;
3. For all possible sets that satisfies 1) and 2), $\bar{S}_a$ has the smallest size. We refer to determining $\bar{S}_a$ as a constrained minimum connected dominating set (constrained MCDS) problem. Note that if $S_a = \phi$, then $\bar{S}_a$ is the MCDS of S. To achieve Ω-DOFT (Ω ≥ 1) in the wireless sensor network, we need to find the set of FT nodes S_t^{Ω} such that $S_t^{\Omega} = \bigcup_{\forall S_f \subseteq S_a, |S_f| \leq \Omega} \mathcal{M}(S \setminus S_f, S_a \setminus S_f)$. Let $N_k^f \subseteq N_k^a$ be the set of failing active neighbors of s_k. We can obtain a lower bound on the number of FT nodes needed to achieve Ω-DOFT (Ω > 1) as follows [32]:

$$\begin{aligned} |S_t^{\Omega}| &= \Big| \bigcup_{\forall |S_f| = \Omega, S_f \subseteq S_a} \bigcup_{s_k \in S_f} N_k^{\Omega} \Big| \geq \Big| \bigcup_{\forall |S_f| \leq \Omega, S_f \subseteq S_a} \left(\bigcup_{\forall s_k \in S_f} \mathcal{M}(N_k \setminus N_k^f, N_k^a \setminus N_k^f) \right) \Big| \\ &\Rightarrow |S_t^{\Omega}| \geq \Big| \bigcup_{\forall |S_f| \leq \Omega, S_f \subseteq S_a} \mathcal{M}(S \setminus S_f, S_a \setminus S_f) \Big| \end{aligned} \tag{7}$$

Note that if Ω = $|S_a|$, $S_a \setminus S_f = \phi$, then $|S_t^{\Omega}| \geq |\mathcal{M}(S \setminus S_a, \phi)|$.

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

4.3. Connectivity-oriented Selection of Fault Tolerance Nodes

Since the CDS and MCDS problems are $\mathcal{NP}$-complete [3,4,8,25,28], finding the constrained MCDS to achieve Ω-DOFT as shown in Equation (7) is also $\mathcal{NP}$-complete. When only single-hop knowledge is available, for any $s_k \in S_a$, there are a total of $\sum_{i=1}^{\Omega} \binom{|N_k^a|}{i}$ possible combinations of failing nodes for s_k; as a result, the total number of possible combination of failing nodes for all the active nodes is $\sum_{\forall s_k \in S_a} \left(\sum_{i=1}^{\Omega} \binom{|N_k^a|}{i} \right)$. Each evaluation requires the finding of the MCDS for neighbors of the failing node. Even though failing active nodes may share many neighbors, a through evaluation in this way is still computationally very expensive.

For a wireless sensor network with a set S_a of active nodes serving as a backbone, the maximum number of nodes that can fail is $|S_a|$. We propose the following distributed procedure to achieve fault tolerance for the simultaneous failure of up to $|S_a|$. The proposed distributed procedure is based on the algorithm from [28]. Note that other heuristics, such as the algorithms described in [3,25], can also be used as the base for building our distributed procedure, since the proposed fault tolerance procedure is a stand-alone module operating on the existing subset of backbone nodes. The procedure contains three steps as shown in Fig. 3.

In Step 1 of Fig. 3, each active node selects a FT node for any of its disconnected active neighbors. We refer to this type of FT nodes as gateway FT nodes since they provide alternative routing paths for active neighbors of the failing node. When that potential failing node actually fails, the network traffic from the failing node to its active neighbors can still be delivered. Though the first type of FT nodes are able to take care of the routing data originating from failing active nodes, they are not necessarily connected among each other and are not necessarily connected to sleeping neighbors of the failing active node. Step 2 in Fig. 3 deals with this problem by using a modified version of the algorithm proposed in [28], which proposed a distributed approach for constructing the CDS for a connected but not a completely connected graph. In the worst case, when all nodes in S_a fail at the same time, the subgraph representing the FT nodes should be a CDS of the subgraph representing S_s. We can therefore utilize the algorithm proposed in [28] with the target graph representing S_s. Note that in Step 2, we have

Distributed FT nodes selection procedure

/* Potential failing node s_k selects gateway FT node */
Step 1. $\forall s_k \in S_a$, for each pair of active neighbors that are not directly connected, s_k selects $s_i \in N_k^s$ as FT node if s_i connects both of them.
/* Ensure that FT nodes are connected */
Step 2. $\forall s_k \in S_s$,
  Step 2.1. if s_k has two disconnected FT neighbors, then s_k assigns itself as FT node;
  Step 2.2. if s_k has two disconnected FT neighbor node and sleeping node, then s_k assigns itself as FT node;
/* Each node must have at least one FT neighbor node. */
Step 3. $\forall s_k \in S_s$, if s_k has no FT neighbors, then s_k assigns itself as FT node.

FIGURE 3 Distributed fault tolerance nodes selection procedure.

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

already found gateway FT nodes, therefore Step 2 needs only check for connectivity of disconnected FT nodes. To ensure that the proposed distributed procedure is also applicable to more general scenarios, Step 3 is added to handle the case that the subgraph representing S_s is a completely connected graph. Let Δ be the maximum node degree. In Fig. 3, Step 1 takes $O(\Delta^3)$ time, Step 2 takes $O(\Delta^2)$ time, and Step 3 takes $O(\Delta)$ time. Therefore, the proposed procedure takes $O(\Delta^3)$ time. We next prove that the proposed distributed procedure achieves $|S_a|$-DOFT for a wireless sensor network with the set of active nodes given by S_a.

Theorem 6. Assume that all nodes in S are connected, i.e., $\forall s_i, S_j \in S$, there exists a routing path from s_i to s_j. Assume that S_a is the set of active nodes as a backbone that keeps all nodes connected. Assume that S_t is the set of FT nodes obtained from the distributed FT selection procedure given by Fig. 3. The set S_t achieves Ω-DOFT in this wireless sensor network, where $\Omega = |S_a|$.

Proof. Since the maximum number of nodes that can fail is $|S_a|$, we only need to consider the case that the selected FT nodes in S_t are able to keep the network fully connected when all nodes in S_a fail. Let $G_s(V_s, E_s)$ be the subgraph representing $S_s = S \backslash S_a$ and $G_t(V_t, E_t)$ be the subgraph representing S_t. To prove that G_t is a CDS of G_s, we first show that G_t is connected, then we show that for any $v \in V_s$, v is either in V_t or adjacent to a vertex in V_t.

Consider any $u, v \in V_t$. Since G_s is connected, $\exists P(u, v)$ as the shortest path from u to v in G_s, where $P(u, v) \subseteq V_s$ is the set of the vertices in the path. If $|P(u, v)| = 2$, the theorem is trivially proved. Assume $|P(u, v)| \geq 3$, and let $P(u, v) = \{u, u_1, u_2, \ldots, v\}$. Consider predecessor vertices of u in $P(u, v)$, i.e., u_1. Since $u \in V_t$, from Step 2 in Fig. 3, u_1 has to be in V_t, irrespective of whether u_2 is in V_t. The same argument holds for u_2. Doing this repeatedly, we have $\forall w \in P(u, v)$, $w \in V_t$, i.e., $P(u, v) \in V_t$. Next, $\forall v \in V_s$, from Step 3 in Fig. 3, v has at least one FT neighbor. Therefore, G_t is a CDS of G_s.

5. Coverage-Centric Fault Tolerance

In Section 4, we have discussed the Ω-DOFT problem for fault-tolerant communication connectivity of up to Ω active nodes failing simultaneously ($\Omega > 1$). However, we should also take fault tolerance for sensing coverage into account to achieve the surveillance goal over the field of interest. This implies that the nodes selected as FT nodes must be able to provide enough sensing coverage over the areas that were originally under the surveillance of the Ω failing active nodes.

5.1. Loss of Sensing Coverage from Failing Nodes

Recall the collective coverage probability for a grid point g_i defined in Section 3. Since only the active nodes in S_a perform communication and sensing tasks, the collective coverage probability for g_i is actually from nodes in S_i^a, where $S_i^a \subseteq S_i$ is the set of active nodes that can detect g_i. When the nodes fail in the network, the set of active nodes that can detect g_i, i.e., S_i^a, changes with time, which subsequently changes the sensing coverage over that grid point. Let $q_i(S)$ be a mapping from a set S of nodes to the coverage probability for grid point g_i, $p_i(t)$ be a mapping from a time instant t to the coverage probability for grid point g_i, and $S(t)$ be a mapping from a time instant t to a set of nodes. Then $S_i(t)$ is the set of nodes that can detect grid point g_i at time instant t. For example, if at time instant t, only nodes in the subset S_i^a, i.e., active nodes, detect grid point g_i, therefore $S_i(t) = S_i^a$ and $p_i(t) = q_i(S_i(t)) = q_i(S_i^a)$. Therefore, from Equation (2), the collective

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

coverage probability of g_i under the fault tolerance constraint is a function of time given as follows:

$$p_i(t) = q_i(S_i^a(t)) = 1 - \prod_{s_k \in S_i^a(t)} (1 - p_i^k), \tag{8}$$

where $S_i^a(t)$ is the set of active nodes that can still detect g_i at time instant t. Therefore, the goal is to ensure that the selected FT nodes and existing active nodes, i.e., $S_a^\Omega = S_a \cup S_t^\Omega$, are able to keep the sensor field adequately covered whenever up to Ω active nodes fail. Thus, successful sensing coverage over the sensor field for FTNS in wireless sensor networks is indicated by:

$$\forall g_i \in \mathcal{G}, \quad p_i(t) \geq p_{th}, \tag{9}$$

where p_{th} is the coverage probability threshold defined in Section 3. Theorem 7 shows the relationship between the loss of sensing coverage and the fault-tolerant operation in wireless sensor networks.

Theorem 7. Assume that all nodes in S are connected, i.e., $\forall s_i, s_j \in S$, there exists a routing path from s_i to s_j. Let $\mathcal{G}$ be the set of all the grid points in the sensor field. Let S_i be the set of nodes that can detect the grid point $g_i \in \mathcal{G}$ initially after the deployment. Let $S_i(t)$ be the set of nodes that can detect g_i at time t, and $S_i^f(t)$ be the set of failing active nodes for g_i at time t. Throughout the operational life time of a sensor network, $\forall g_i \in \mathcal{G}$, the following must be satisfied for any time instant t:

$$p_f(t+1) \leq \frac{p_i(t) - p_{th}}{1 - p_{th}}. \tag{10}$$

where $p_i(t) = 1 - \prod_{s_k \in S_i(t)} (1 - p_i^k)$ *and* $p_f(t+1) = 1 - \prod_{s_k \in S_i^f(t+1)} (1 - p_i^k)$.

Proof. Consider time instants t and $t + 1$. Obviously we have $S_i(t) \subseteq S_i$ and $S_i(t) = S_i(t+1) \cup S_i^f(t+1)$. From Equation (8), we have

$$\begin{aligned} p_i(t) = 1 - \prod_{s_k \in S_i(t)} (1 - p_i^k) &= 1 - \prod_{s_k \in S_i(t+1) \cup S_i^f(t+1)} (1 - p_i^k) \\ &= 1 - \prod_{s_k \in S_i(t+1)} (1 - p_i^k) \prod_{s_k \in S_i^f(t+1)} (1 - p_i^k). \end{aligned}$$

Similarly, $p_i(t+1) = 1 - \prod_{s_k \in S_i(t+1)} (1 - p_i^k)$. Let $p_f(t) = 1 - \prod_{s_k \in S_i^f(t)} (1 - p_i^k)$ and $p_f(t+1) = 1 - \prod_{s_k \in S_i^f(t+1)} (1 - p_i^k)$. Then we have

$$p_i(t) = 1 - (1 - p_i(t+1))(1 - p_f(t+1)) = p_f(t+1) + p_i(t+1)(1 - p_f(t+1)).$$

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

Therefore, $p_i(t+1) = \dfrac{p_i(t) - p_f(t+1)}{1 - p_f(t+1)}$. From Equation (9), which expresses the FTNS sensing coverage condition for any time instant, we have $p_i(t+1) \geq p_{th} \Rightarrow \dfrac{p_i(t) - p_f(t+1)}{1 - p_f(t+1)} \geq p_{th}$, which implies that $p_f(t+1) \leq \dfrac{p_i(t) - p_{th}}{1 - p_{th}}$. ■

From the proof of Theorem 7, we see that $p_f(t + 1)$ represents the sensing coverage loss at time $t + 1$ at grid point g_i caused by the failing nodes in $S_i^f(t+1)$. To satisfy the coverage probability threshold requirement, $p_f(t + 1)$ must not exceed $\dfrac{p_i(t) - p_{th}}{1 - p_{th}}$. In other words, if we can bound the coverage loss $p_f(t)$ below $\dfrac{p_i(t) - p_{th}}{1 - p_{th}}$ during the operational lifetime of the sensor network for all grid points on the field, the sensor network is able to tolerate up to Ω nodes failing simultaneously. When $p_i(t)$ drops, the bound on the coverage loss from failing nodes at the next time instant, i.e., $p_f(t + 1)$, becomes tighter since $\dfrac{p_i(t) - p_{th}}{1 - p_{th}}$ decreases when $p_i(t)$ decreases. This can also be used as a warning criteria to inform the base station whether a current node may lose sensing coverage over its sensing area.

Note that the fault tolerance problem for sensing coverage differs from the fault tolerance problem for communication connectivity discussed in Section 4 since there is no direct relationship between the number of failing nodes and the coverage loss $p_f(t)$. For example, for g_i with $|S_i(t)| = 1$, $p_i(t)$ might be the same as $p_j(t)$ for g_i where $|S_j(t)| = 1, 2, 3$ or even higher. This is due to the fact that for any grid point g_i, $p_i(t)$ is not directly related to the number of nodes that can detect g_i but rather to the distances from these nodes to g_i, as defined by Equation (1).

5.2. Distributed Approach

We next propose a coverage-centric fault tolerance algorithm that can be executed in a distributed manner, and requires much less computation than the centralized case. Without loss of generality, assume $r_c \geq 2r_s$, i.e., $S_i \subseteq N_k$. For grid point $g_i \in A_k$ corresponding to node $s_k \in S_i^a \subseteq S_a$, the maximum coverage loss happens when all nodes in S_i^a fail. In this case, the coverage loss for g_i, denoted as $q_i(S_i^a)$, is given as $q_i(S_i^a) = 1 - \prod_{s_k \in \cup S_i^a} (1 - p_i^k)$. Let $S_i^\Omega \subseteq S_i^s$ be the set of FT nodes for grid point g_i. The coverage compensation from S_i^Ω, denoted as $q_i(S_i^\Omega)$, is given as $q_i(S_i^\Omega) = 1 - \prod_{s_k \in S_i^\Omega} (1 - p_i^k)$. Let $q_i(S_i^a \cup S_i^\Omega)$ be the coverage from both active nodes and the FT nodes for g_i. Similarly, $q_i(S_i^a \cup S_i^\Omega) = 1 - \prod_{s_k \in S_i^a \cup S_i^\Omega} (1 - p_i^k)$. Assuming that the maximum coverage loss happens at time instant $t + 1$, i.e., $S_i(t) = S_i^a \cup S_i^\Omega, S_i(t+1) = S_i^\Omega$, and $S_f(t+1) = S_i^a$, then accordingly, we have corresponding expression as $p_i(t) = q_i(S_i^a \cup S_i^\Omega), p_i(t+1) = q_i(S_i^\Omega)$ (1), and $p_f(t+1) = q_i(S_i^a)$. From Equation (10), if the following is satisfied for all grid points in the sensing area of s_k, i.e., A_k, then the node s_k is able to tolerate the maximum

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

number of failing active nodes within its own sensing area without losing sensing coverage:

$$p_f(t+1) \le \frac{p_i(t) - p_{th}}{1 - p_{th}} \Rightarrow q_i(S_i^a) \le \frac{q_i(S_i^a \cup S_i^\Omega) - p_{th}}{1 - p_{th}}, \quad \forall g_i \in A_k. \tag{11}$$

Equation (11) requires $\sum_{j=1}^{|S_i^s|} \binom{|S_i^s|}{j}$ evaluations for a total of $|A_k|$ grid points within s_k's sensing area. When each active node executes the evaluation procedure described by Equation (11), the maximum total number of evaluations is $\sum_{g_i \in \mathcal{G}} \sum_{j=1}^{|S_i^s|} \binom{|S_i^s|}{j}$. However, note that $q_i(S_i^a \cup S_i^\Omega) = q_i(S_i^a) + q_i(S_i^\Omega) - q_i(S_i^a) q_i(S_i^\Omega)$, therefore, from Equation (11), we have

$$q_i(S_i^a) \le \frac{q_i(S_i^a \cup S_i^\Omega) - p_{th}}{1 - p_{th}} \Rightarrow q_i(S_i^\Omega) \ge p_{th}, \tag{12}$$

which corresponds to the analysis in Theorem 7. Equation (12) implies that we can design the fault-tolerance nodes selection for sensing coverage in a much less computationally expensive way. Figure 4 shows the pseudocode for the coverage-centric fault tolerance node selection algorithm.

As shown in Fig. 4, to select the minimum number of FT nodes without a thorough evaluation over all subsets of nodes in S_i^s, we first construct L_i from S_i^s, where L_i is a list corresponding to the set of nodes S_i^s such that L_i is constructed as a sorted list in the descending order of the individual coverage on grid point g_i of all nodes in S_i^s. For any $s_k \in S_i^s$, the corresponding element in L_i is denoted by $l(s_k)$, which gives the position of s_k in the list L_i. Therefore, for any two different nodes $s_{k_1}, s_{k_2} \in S_i^s, l(s_{k_1}) \le l(s_{k_2})$ if

Procedure *DistCovCentricFTNSelection* (s_k)

```
01 Set S_k^Ω = φ;
02 For ∀g_i ∈ A_k /* Check if current FT nodes in S_k^Ω are adequate for fault tolerance at g_i. */
03     If q_i(S_k^Ω) > p_th  Continue;  End /* Find FT nodes, i.e., S_i^Ω, for g_i. */
04     Construct the sorted list L_i from S_i^s;
05     For j = |L_i| to 1
06         If q_i(L_i(1, ··· , j)) ≥ p_th  Continue;  End
07         If j == |L_i|  break;  End /* Not enough nodes in S_i^s for fault-tolerance. */
08         Set S_k^Ω = L_i(1, ··· , j + 1);  Break;
09     End
10 End
```

FIGURE 4 Pseudocode for the distributed coverage-centric fault tolerance nodes selection.

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

$p_i^{k_1} \geq p_i^{k_2}$. We denote the length of the list L_i as $|L_i|$, where $|L_i| = |S_i^s|$. We define the position $l(s_k)$ as a positive integer, where $l(s_k) = 1$ if s_k is the first element in L_i and $l(s_k) = |L_i|$ if s_k is the last element in L_i. We refer to a subset containing a single node s_k in L_i at the j-th position by $L_i(j)$, i.e., $L_i(j) = \{s_k | l(s_k) = j,\ 1 \leq j \leq |L_i|\}$. Furthermore, we use $L_i(j_1, j_2, \ldots, j_u)$ to denote the subset of nodes $\{s_{k_1}, s_{k_2}, \cdots, s_{k_u} | l(s_{k_1}) = j_1, l(s_{k_2}) = j_2, \cdots, l(s_{k_u}) = j_1 \text{ and } 1 \leq j_1 \leq j_2 \leq \cdots \leq j_u \leq |L_i|\}$. Thus, for a given grid point g_i, when there are enough nodes in S_i^s for g_i as FT nodes, Fig. 4 is able to generate the subset of FT nodes from S_i^s with the minimum number of FT nodes among for g_i. Note however that to avoid the repeated selection of the same nodes for different grid points, before selecting the FT nodes for the current grid point, the coverage support from existing FT nodes in S_i^Ω is checked first to see if they already provide enough coverage support when active nodes fail; see line 3 in Fig. 4. Therefore, even though the number of FT nodes selected is locally minimum for a given grid point, it is not necessarily a global minimum.

Note that the evaluation procedure is per grid point, which can be executed on either a sleeping node or an active node. For any $g_i \in \mathcal{G}$, only one node needs to perform the selection of FT nodes for g_i. This implies that the total number of nodes required for executing such evaluation procedure is $\left\lceil \frac{|\mathcal{G}|}{|A_k|} \right\rceil$ or $\left\lceil \frac{A}{\pi r_s^2} \right\rceil$ where A is the area of the surveillance field (assuming that either $r_c \geq 2r_s$ or $\left\lceil \frac{2r_s}{r_c} \right\rceil$ -hop knowledge is available). Also note that in Fig. 4, there is no need to calculate $q_i(S_i^a)$ every time since it is available from the previous stage when S_a is determined. Further computation can be reduced by temporarily storing the $q_i(S_k^\Omega)$ for the current grid point for evaluation at the next grid point, where $q_i(S_i^\Omega \cup S_k^\Omega)$ can be obtained as: $q_i(S_i^\Omega \cup S_k^\Omega) = q_i(S_i^\Omega) + q_i(S_k^\Omega) - q_i(S_i^\Omega) q_i(S_k^\Omega)$.

The sorting procedure needed to construct L_i from S_i^s has a time complexity of $O(\Delta \log \Delta)$, where Δ is the maximum node degree. The pseudocode between line 5 to line 9 in Fig. 4 for FT nodes selection has a time complexity of $O(\Delta)$. Since the distributed coverage-centric fault-tolerant procedure in Fig. 4 is carried out per grid point, the overall time complexity for the distributed coverage-centric fault-tolerant node selection has a time complexity as $O(m\Delta(1 + \log \Delta)) = O(m\Delta \log \Delta)$, where m is the number of grid points. The next theorem shows that the procedure of Fig. 4 leads to the smallest number of FT nodes needed to satisfy the coverage threshold for a given grid point g_i. The proof is given in the appendix.

Theorem 8. For a grid point g_i, the distributed coverage-centric fault-tolerance node selection procedure given by the pseudocode in Fig. 4 gives the minimum number of fault-tolerance node.

As shown in Figs. 3 and 4, the proposed scheme does not require a centralized server to determine backup nodes for the existing backbone. FT nodes are designated in a distributed fashion; this procedure requires only localized communication (single-hop or restricted hop communication between nodes). The proposed self-organization approach for fault tolerance is therefore scalable, which makes it suitable for ad hoc sensor networks with a large number of deployed nodes.

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

6. Simulation and Discussion

We have implemented CCANS in ns2 and integrated as a module in the ESP AESOP protocol. The Emergent Surveillance Plexus (ESP) [34] is a Multi-disciplinary University Research Initiative (MURI), whose goal is to advance the surveillance capabilities of wireless sensor networks. It involves participants from Pennsylvania State University, University of California at Los Angles, Duke University, University of Wisconsin, Cornell University, and Louisiana State University. AESOP stands for *An Emergent-Surveillance-Plexus Self-Organizing Protocol*, which is designed for target tracking in wireless sensor networks with high tracking quality and energy efficiency [5]. A more detailed description of the AESOP protocol can be found in [5].

6.1. Simulation Results

In a simulation for the proposed fault-tolerant self-organization algorithms, we first collect the data from the distributed CCANS procedure described in Section 3. We next evaluate the proposed distributed FTNS procedure using MatLab by feeding the data collected from CCANS as inputs. The data from CCANS contains locations of sensor nodes after deployment and their final state decisions. There are 150, 200, 250, 300, 350, and 400 nodes in each random deployment, respectively, on a 50×50 grid representing a 50m $\times$ 50m sensor field. All nodes have the same maximum communication radius r_c = 20m and maximum sensing range r_s = 10m. The value of Ω is set to the number of active nodes. Figures 5–8 show the simulation results for distributed fault-tolerance self-organization procedure.

Figure 5(b)(i) shows the results obtained for connectivity-oriented selection of FT nodes. Note that the percentage of FT nodes decreases nearly at the same rate as the percentage of active nodes. This is because the connectivity-oriented FT nodes selection algorithm is executed in a distributed manner and each node uses only one-hop knowledge. Note also that the percentage of FT nodes is lower than the percentage of active nodes determined by CCANS. This is because CCANS considers both communication connectivity and sensing coverage in selecting active nodes. Figure 5(b)(ii) shows the results for coverage-centric selection of FT nodes. Since the coverage-centric fault-tolerance nodes selection procedure given by Fig. 4 has been proven to generate the minimum number of fault-tolerance nodes, the percentage shown in Fig. 5(b)(ii) is much lower than the percentage of active nodes from CCANS.

The distributed fault-tolerance nodes selection procedure contains two stages. We consider two cases for the implementation, namely "FTNS-1" and "FTNS-2". FTNS-1 refers to the case that the first stage is the coverage-centric selection of fault-tolerance nodes (FTNS-1 Stage 1) and the second stage is the connectivity-centric selection of FT nodes (FTNS-1 Stage 2). FTNS-2 refers to the case that the first stage is the connectivity-centric selection of FT nodes (FTNS-2 Stage 1) and the second stage is the coverage-centric selection of FT nodes (FTNS-2 Stage 2). Figure 5(a) presents the result for the distributed FTNS algorithm. In both FTNS-1 and FTNS-2, the FT nodes that have already been selected in Stage 1 are checked first in Stage 2 to see if they already provide enough sensing coverage for fault tolerance. This decreases the number of FT nodes needed for Stage 2 of coverage-centric FT nodes selection, which is shown in Fig. 5(a). Note that in Fig. 5(a)(ii), the percentage of FT nodes in Stage 1 is

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

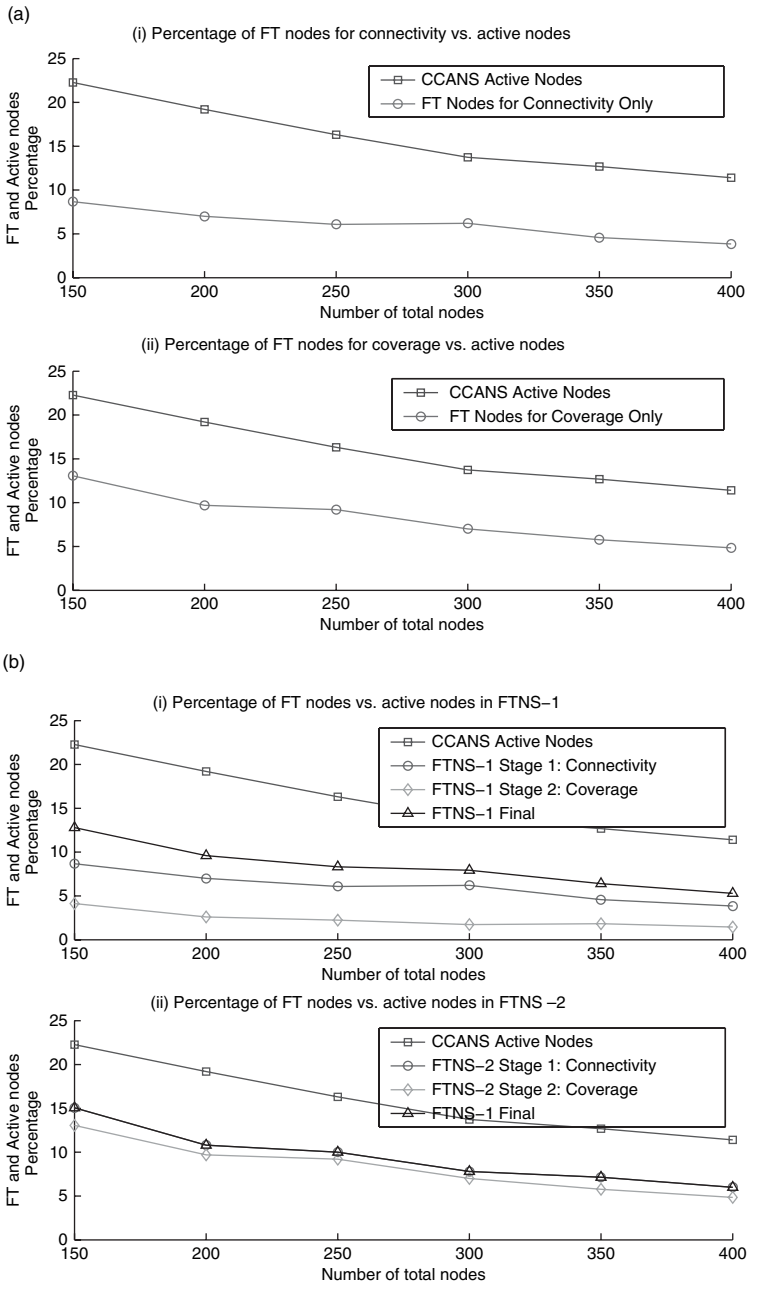


FIGURE 5 Simulation results: (a) Percentage of FT nodes: (i) FT nodes for connectivity only; (ii) FT nodes for coverage only. (b) Percentage of FT nodes for the distributed FTNS procedure (with both coverage and connectivity concerns): (i) FTNS-1: Stage 1 selects FT nodes for coverage and FTNS Stage 2 selects FT nodes for connectivity; (ii) FTNS-2 Stage 1 selects FT nodes for connectivity and FTNS Stage 2 selects FT nodes for coverage.

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

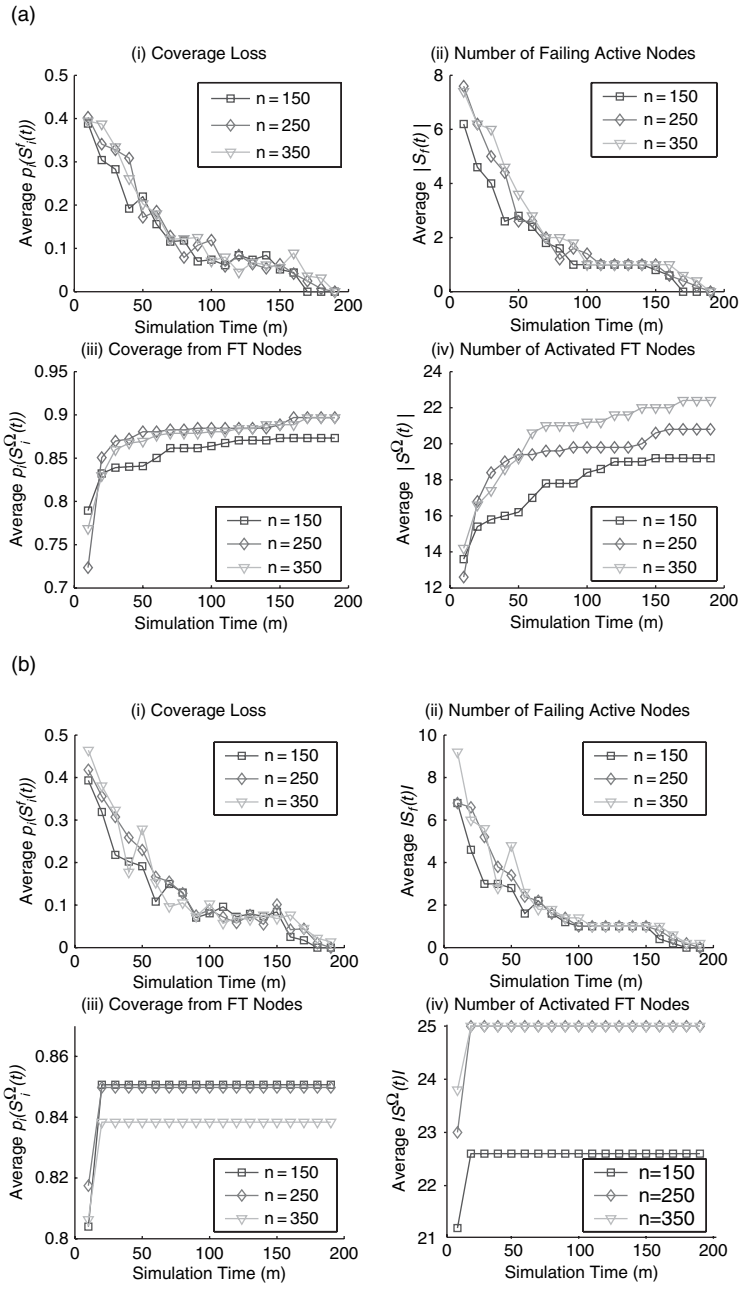


FIGURE 6 Simulation results: (a) Effect of failing active nodes vs. activated FT nodes for FTNS-1: (i) Average coverage loss from failing active nodes; (ii) Average number of activated FT nodes; (iii) Average coverage loss from failing active nodes; (iv) Average number of activated FT nodes; (b) Effect of failing active nodes vs. activated FT nodes for FTNS-2: (i) Average coverage loss from failing active nodes; (ii) Average number of activated FT nodes; (iii) Average coverage loss from failing active nodes; (iv) Average number of activated FT nodes.

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

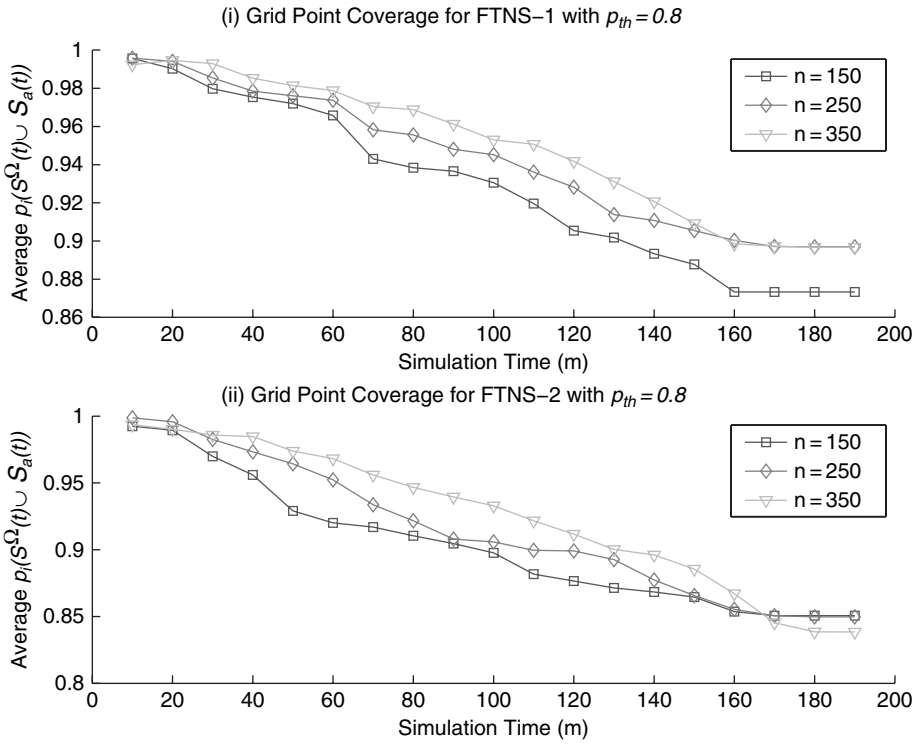


FIGURE 7 Average grid point coverage when active nodes fail during the simulation.

the same as the percentage of FT nodes at the end of the FTNS procedure. This is due to the fact that we have $r_c = 2r_s$ in this scenario. As shown in [31], when $r_c = 2r_s$, the connectivity is automatically guaranteed by the subset of nodes needed to maintain the sensing coverage.

Next, we simulate the failing of active nodes to show that FT nodes are able to provide the coverage and connectivity when active nodes fail. This is shown in Fig. 6. The sensor network layout and configuration are the same as those in Fig. 5. We use a simplified model for generating the failing active nodes. For a total simulation time of 200 minutes, we select a random number of active nodes from the currently alive active nodes every 10 minutes, and assign them as failing nodes. The neighboring FT nodes determine that these nodes have failed. As shown in Fig. 6, the failing of active nodes leads to an activation of the designated FT neighbors. The loss of coverage from the failing active nodes are compensated by the coverage support from the activated FT nodes. The simulation stops when all active nodes have failed. Fig. 7 shows the change in coverage probability for grid points in the sensor field. Note that the average grid point coverage probability decreases with time. This is due to the fact that the coverage-centric FT nodes selection only selects the minimum number of FT nodes to save energy; the goal is not to maximize the coverage. However, at any time instant, the coverage probability is always higher than the required coverage probability threshold $p_{th} = 0.8$. Also note that at any time instant, the connectivity is guaranteed by the activated FT nodes and alive active nodes for both FTNS-1 and FTNS-2.

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

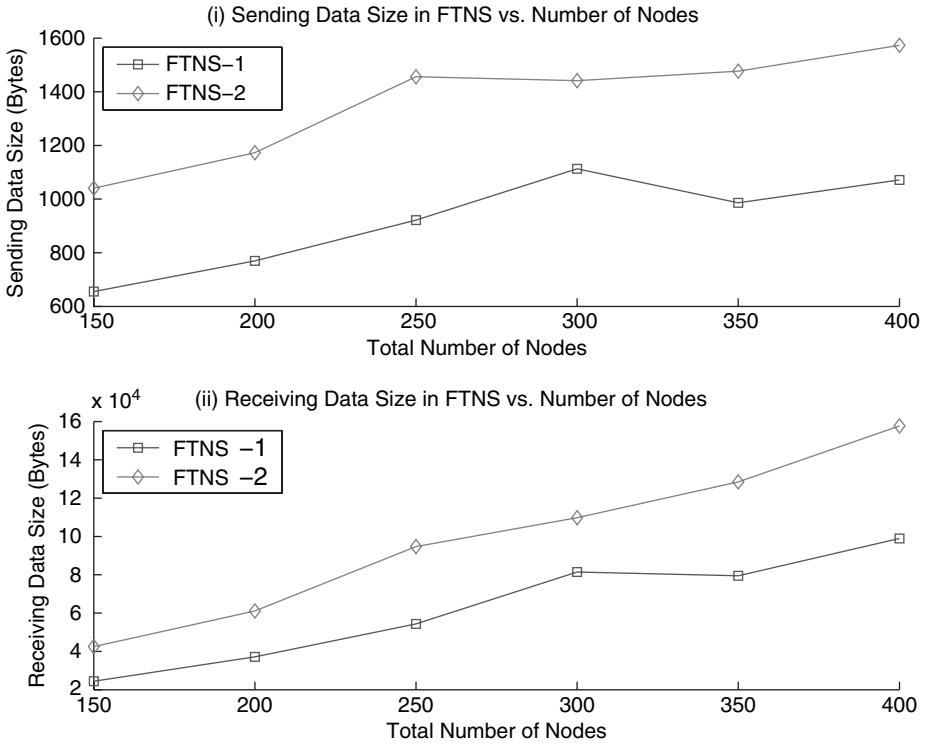


FIGURE 8 Communication data message size in FTNS for FT nodes selection.

6.2. Discussion

Note that upper bounds on the number of the fault-tolerance node given in previous sections are important because they can be used as a guideline for the initial sensor nodes deployment to achieve fault-tolerant self-organization. For example, as shown by Fig. 5, we can deploy the number of sensor nodes that are sufficient enough to provide the required level of fault tolerance in the sensor network. The lower bound on the number of fault-tolerance node is useful since it can be used as a baseline for comparing different heuristics. Note that the problem of finding a minimum connected dominating set (MCDS) for a general graph is a $\mathcal{NP}$-complete and it is hard to approximate. The original work of using MCDS as a backbone for routing by Bharghavan and Das in [4] has a approximation ratio of $3H(\Delta)$, where Δ is the maximum node degree and $H(\Delta)$ is the Δth Harmonic number given $H(\Delta) = \sum_{i=1}^{\Delta} \frac{1}{i}$. A comparison of recent distributed algorithms for forming CDS described in [3,25,28] can be found in [3]. In this paper, we used the distributed algorithm proposed in [28] for its simplicity of implementation. However, the proposed fault-tolerance procedure in this paper is not limited by any particular heuristics for backbone nodes selection to form CDS. In our case, the lower bound is not on the set of all nodes but the subset of nodes that are not selected as backbone nodes, i.e., candidate fault-tolerance nodes. This is referred to as the constrained minimum connected dominating set problem in our paper. Therefore, heuristics in existing literatures such as [3,4,25,28] can be directly used to obtain the approximations of MCDS by only applying it on the subset of non-backbone nodes.

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

The proposed distributed fault-tolerance nodes selection procedure is a localized algorithm. Localized algorithms are considered as a special type of distributed algorithms where only a subset of nodes in the wireless sensor networks participate in sensing, communication, and computation [18]. For either stage in the proposed distributed fault-tolerance nodes selection procedure, it requires only local knowledge and constant rounds of communication for message exchange among the neighborhood. From the discussion in Subsection 4.3 and 5.2, the total time complexity for the distributed FTNS is $O(m\Delta \log\Delta + \Delta^3)$. For message complexity, both stages in FTNS require the exchange of a constant number of messages within the neighborhood. The active nodes in the backbone first carries out the computation for connectivity checking and coverage evaluation to select a subset of nodes from its sleeping neighbors, then it broadcasts the list of selected FT neighbors within its neighborhood. The designated FT nodes need not be activated until the active nodes fail. In Fig. 8, we show the evaluation of communication data size for FT nodes selection.

In FT nodes selection, active nodes send the message containing the list of node ids of the designated FT neighbors. Neighbors of active nodes search the received id list and set themselves as FT nodes for that active node, i.e., FT nodes that can be activated into an active state by their failing active neighbors. The designated FT nodes then send an acknowledge message back to the active nodes to confirm the FT node assignment. Assuming that there is no packet loss, this takes 2 rounds of communication within the neighborhood of active odes. The message size complexity is then $O(\Delta)$. For the activation of FT nodes, we assume that designated FT nodes periodically poll their active neighbors about whether they are still alive or not. The polling frequency depends on the sensor network application requirement and sensor nodes failure distribution, since it should not require excessive energy and bandwidth. The problem of determining the polling frequency is not considered in this paper. Note that it is possible to simply let all sleeping nodes do the polling without designating any fault-tolerance nodes. However, this also means that when an active node fails, all its sleeping neighbors have to become active. This adversely affects the potential of extending the lifetime for the densely deployed sensor network. Figure 8 shows the average communication data size for both FTNS-1 and FTNS-2.

7. Conclusions

In this paper, we have investigated fault tolerance for coverage and connectivity in wireless sensor networks. Fault tolerance is necessary to ensure robust operation for surveillance and monitoring applications. Since wireless sensor networks are made up of inexpensive nodes and they operate in harsh environments, the likely possibility of node failures must be considered. We have characterized the amount of redundancy required in the network for fault tolerance. Based on an analysis of the redundancy necessary to maintain communication connectivity and sensing coverage, we have proposed the distributed FTNS algorithm for fault-tolerant self-organization. FTNS is able to provide a high degree of fault tolerance such that even when all of these active nodes fail simultaneously, the coverage and the connectivity in the network are not affected. The proposed distributed FTNS approach is scalable and requires only localized communication. We have implemented FTNS in MatLab and presented representative simulation results.

About the Authors

Yi Zou received the B.E. in Electrical Engineering from Si Chuan University, P. R. China, in 1997, the M.E. in Electrical Engineering from Nanyang Technological University,

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

Singapore, in 2000, and Ph.D. in Computer Engineering from Duke University in 2004. Upon completion of his Ph.D. he worked as a Research Associate at Duke University. Since August 2005, he is with Unitrends Software Corp., Columbia, SC, where he is responsible for developing networked backup/restore systems. Before his Ph.D. program, he was working as a development engineer for VPN products at CE-Infosys Pte. Ltd., Singapore. In the summer of 2003, he was an intern at Xerox PARC, Palo Alto, CA. From He worked as a Research Associate in the Electrical and Computer Engineering Department at Duke University at Durham, NC, U.S.A. His research interests include ad hoc networks, wireless communication, embedded system computing, and robotics. He has published 21 technical papers, and served as an organization committee member for {IEEE WICON'05 Workshop}, and technical committee member for {IEEE ICWMC' 06}.

Krishnendu Chakrabarty received the B. Tech. degree from the Indian Institute of Technology, Kharagpur, in 1990, and the M.S.E. and Ph.D. degrees from the University of Michigan, Ann Arbor, in 1992 and 1995, respectively, all in Computer Science and Engineering. He is now Professor of Electrical and Computer Engineering at Duke University. Prof. Chakrabarty is a recipient of the National Science Foundation Early Faculty (CAREER) award and the Office of Naval Research Young Investigator award. His current research projects include: testing and design-for-testability of system-on-chip integrated circuits; microfluidic biochips; microfluidics-based chip cooling; wireless sensor networks. Prof. Chakrabarty has authored five books—*Microelectrofluidic Systems: Modeling and Simulation* (CRC Press, 2002), *Test Resource Partitioning for System-on-a-Chip* (Kluwer, 2002), *Scalable Infrastructure for Distributed Sensor Networks* (Springer, 2005), *Digital Microfluidics Biochips: Synthesis, Testing, and Reconfigutaion Techniques* (CRC Press, 2006), and *Adaptive Cooling of Integrated Circuits using Digital Microfluidics* (Artech House, April 2007)—and edited the book volumes *SOC (System-on-a-Chip) Testing for Plug and Play Test Automation* (Kluwer, 2002) and *Design Automation Methods and Tools for Microfluidics-Based Biochips* (Springer, 2006). He has contributed over a dozen invited chapters to book volumes, and published 250 papers in archival journals and refereed conference proceedings. He holds a US patent in built-in self-test and is a co-inventor of a pending US patent on sensor networks. He is a recipient of best paper awards at the 2007 *IEEE International Conference on VLSI Design*, the 2005 *IEEE International Conference on Computer Design*, and the 2001 *IEEE Design, Automation and Test in Europe (DATE) Conference*. He is also a recipient of the Humboldt Research Fellowship, awarded by the Alexander von Humboldt Foundation, Germany, and the Mercator Visiting Professorship, awarded by the Deutsche Forschungsgemeinschaft, Germany.

Prof. Chakrabarty is a Distinguished Visitor of the IEEE Computer Society for 2006–2007 and a Distinguished Lecturer of the IEEE Circuits and Systems Society for 2006–2007. He is an Associate Editor of *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on VLSI Systems, IEEE Transactions on Circuits and System I, IEEE Transactions on Biomedical Circuits and Systems, ACM Journal on Emerging Technologies in Computing Systems*, an Editor of *IEEE Design & Test of Computers*, and an Editor of *Journal of Electronic Testing: Theory and Applications (JETTA)*. He is a member of the editorial board for *Microelectronics Journal, Sensor Letters*, and *Journal of Embedded Computing*, and he serves as a subject area editor for the *International Journal of Distributed Sensor Networks*. In the recent past, he has also served as an Associate Editor of *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*. He is a senior member of IEEE, a senior member of ACM, and a member of Sigma Xi. He serves as the chair of the emerging technologies subcommittee for the *IEEE Int. Conf. CAD* (2005–2007), the subcommittee for new, emerging, and specialized technologies for the *IEEE/ACM Design Automation Conference*

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

(2006–2007), and the subcommittee on BIST/DFT for the *IEEE/ACM Design, Automation and Test in Europe (DATE) Conference* (2008). He served as Tutorials Chair for the 2005 *IEEE International Conference on VLSI Design*, Program Chair for the 2005 *IEEE Asian Test Symposium*, and Program Chair for the *CAD, Design, and Test Conference* for the 2007 *IEEE Symposium on Design, Integration, Test, and Packaging of MEMS/MOEMS* (DTIP'07). He delivered keynote talks at the *International Conference & Exhibition on Micro Electro, Opto, Mechanical Systems and Components* (Munich, Germany, October 2005), the *International Conference on Design and Test of Integrated Systems* (Tunis, Tunisia, September 2006), the *IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems* (Krakow, Poland, April 2007), the *IEEE International Symposium on VLSI* (Porto Alegre, Brazil, May 2007), as well as invited talks and tutorials at several other conferences.

References

1. J. R. Agre and L. P. Clare, "An integrated architecture for cooperative sensing networks," *IEEE Computer Magazine*, vol. 33, no. 5, pp. 106–108, 2000.
2. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.
3. K. M. Alzoubi, P. J. Wan, and O. Frieder, "Distributed heuristics for connected dominating sets in wireless ad hoc networks," *J. Communications and Networks*, vol. 4, no. 1, pp. 1–8, 2002.
4. V. Bharghavan and B. Das, "Routing in ad hoc networks using minimum connected dominating sets," *Proc. IEEE ICC*, pp. 376–380, 1997.
5. P. Biswas and S. Phoha, "A Sensor network test-bed for an integrated target surveillance experiment," *Proc. IEEE Conf. Local Computer Networks*, pp. 552–553, 2004.
6. S. Chessa and P. Santi, "Crash faults identification in wireless sensor networks," *Computer Communications*, vol. 25, no. 14, pp. 1273–1282, 2002.
7. D. Estrin, L. Girod, G. Pottie, and M. Srivastava, "Instrumenting the world with wireless sensor networks," *Proc. Intl. Conf. Acoustics, Speech, and Signal Processing*, vol. 4, pp. 2033–2036, 2001.
8. M. R. Garey and D. S. Johnson, *Computers and Intractability: A guide to the theory of NP-completeness*, W. H. Freeman and Co., 1979.
9. S. S. Iyengar, M. B. Sharma, and R. L. Kashyap, "Information routing and reliability issues in distributed sensor networks," *IEEE Trans. Signal Processing*, vol. 40, no. 2, pp. 3012–3021, 1992.
10. F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli, "Fault tolerance in wireless ad-hoc sensor networks," *Proc. IEEE Sensors*, 2002.
11. M. Krasniewski, P. Varadharajan, B. Rabeler, S. Bagchi, and Y. C. Hu, "TIBFIT: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks," *Proc. Intl. Conf. Dependable Systems and Networks (DSN)*, 2005.
12. B. Krishnamachari and S. S. Iyengar, "Distributed Bayesian algorithms for fault-tolerant event region detection in wireless sensor networks," *IEEE Trans. Computers*, vol. 53, pp. 241–250, March 2004.
13. C. Gui and P. Mohapatra, "Power conservation and quality of surveillance in target tracking sensor networks," *Proc. ACM/IEEE MobiCom*, pp. 129–143, 2004.
14. H. Gupta, S. R. Das, and Quinyi Gu, "Connected sensor cover: self-organiziation of sensor networks for efficient query execution," *Proc. IEEE/ACM MobiHoc*, pp. 189–200, 2003.
15. X. Y. Li, P. J. Wan, Y. Wang, and C. W. Yi, "Fault tolerant deployment and topology control in wireless networks," *Proc. ACM/IEEE MobiHoc*, pp. 117–128, 2003.
16. S. Lindsey and C. S. Raghavendra, "PEGASIS: power-efficient gathering in sensor information systems," *Proc. IEEE Aerospace Conf.*, vol. 3, pp. 1125–1130, 2002.
17. K. Marzullo, "Implementing fault-tolerant sensors," *Technical Report 89–997*, Computer Science Department, Cornell University, 1989.
18. S. Meguerdichian, S. Slijepcevic, V. Karayan, and M. Potkonjak, "Localized algorithms in wireless ad-hoc networks: location discovery and sensor exposure," *Proc. MobiHoc*, pp. 106–116, 2001.

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

19. S. Olariu and A. Y. Zomaya, "An overview of mobile communications and computing," in *State of the Art Series*, A. E. Abdallah (Ed), Heidelberg: Springer Verlag, 2004.
20. J. Polastre, J. Hill and D. Culler, "Versatile low power media access for wireless sensor networks," *Proc. ACM SenSys*, pp. 95–107, 2004.
21. L. Prasad, S. S. Iyengar, R. L. Rao, and R. L. Kashyap, "Fault- tolerant sensor integration using multiresolution decomposition," *Physical Rev. E*, vol. 49, no. 4, 1994.
22. L. Schwiebert, S. D. S. Gupta, and J. Weinmann, "Research challenges in wireless networks of biomedical sensors," *Proc. ACM/IEEE MobiCom*, pp. 151–165, 2001.
23. K. Seada, M. Zuniga, A. Helmy, and B. Krishnamachari. "Energy-efficient forwarding strategies for geographic routing in lossy wireless sensor networks," *Proc. ACM SenSys*, pp. 108–121, 2004.
24. D. P. Siewiorek and R. S. Swarz, *Reliable Computer Systems: Design and Evaluation*, MA: A. K. Peters, 1998.
25. I. Stojmenovic, M. Seddigh, and J. Zunic, "Dominating sets and neighbor elimination based broad-casting algorithms in wireless networks," *Proc. IEEE Conf. System Sciences*, 13(1), pp. 14–15, 2002.
26. A. Wang, W. B. Heinzelman, and A. P. Chandrakasan, "Energy-scalable protocols for battery-operated micro sensor networks," *IEEE Workshop on Signal Processing Systems*, pp. 483–490, 1999.
27. X. R. Wang, G. L. Xing, Y. F. Zhang, C. Y. Lu, R. Pless, and C. Gill, "Integrated coverage and connectivity configuration in wireless sensor networks," Proc. *Proc. ACM SenSys*, pp. 28–39, 2003.
28. J. Wu, "Extended dominating-set-based routing in ad hoc wireless networks with unidirectional links," *IEEE Transactions on Parallel and Distributed Computing*, vol. 22, 1–4, pp. 327–340, 2002.
29. Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing," *Proc. ACM/IEEE MobiCom COnference*, pp. 70–84, 2001.
30. F. Xue and P. R. Kumar, "The number of neighbors needed for connectivity of wireless networks," *Wireless Networks* vol. 10, no. 2, pp. 169–181, 2004.
31. Y. Zou and K. Chakrabarty, "A distributed coverage- and connectivity-centric technique for selecting active nodes in wireless sensor networks," *IEEE Trans. Computers*, vol. 54, pp. 978–991, August 2005.
32. Y. Zou and K. Chakrabarty, "Fault-tolerant Self-Organization in Wireless Sensor Networks," *Proc. IEEE DCOSS/Lecture Notes in Computer Science LNCS 3560*, pp. 191–205, Springer, New York, 2005.
33. Crossbow Technology, *http://www.xbow.com/Products/products.htm*, page accessed on April 20, 2006.
34. Emergent Surveillance Plexus (ESP): A multidisciplinary university research initiative (MURI), *http://strange.arl.psu.edu/ESP*, page accessed on April 20, 2006.

Appendix

Proof of Theorem 2

Proof. Since the nodes in N_k are connected, we know from Theorem 1 that at most 10 nodes are needed to keep all nodes in N_k connected if s_k fails. Moreover, active neighbors of s_k are connected to all other neighbors of s_k; since $\Omega = 1$, a routing path from any neighbor inside communication region of s_k to any nodes outside s_k is not broken. Therefore, communication fault tolerance is maintained if s_k fails. ■

Proof of Corollary 1

Proof. Since $|S_a| > 1$, $\forall s_k \in S_a$, $\Delta_k^a \geq 1$. Since $\Delta_k^a > 0$, i.e., $N_k^a \neq \phi$, let us assume that $s_i \in N_k^a$. Then s_i is in one of the six sector areas shown in Fig. 2(a). Based on the proof of Theorem 1, starting from s_i, we need at most 9 more nodes to keep all nodes in N_k connected. As we do not know the locations of the active neighbors inside the sectors in

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

Fig. 2(a), it is possible that all active neighbors of s_k are located close to each other. In this case, when s_k fails, all 9 FT nodes are needed. ■

Proof of Theorem 3

Proof. Let $N_k^1 \subseteq N_k^s$ be the set of FT neighbor nodes for s_k in a 1-DOFT sensor network. If $|V_a| = 1$, then S_a contains only one active node. Assume $S_a = \{s_k\}$. Then $|S_t^1| = |N_k^1| = \Gamma_k$. From Theorem 1, $\forall s_k \in S_a$, it is sufficient to have $\Gamma_k = 10$ for the fault-tolerant communication connectivity within the communication region of s_k. Furthermore, note that If $|V_a| > 1$, then $\forall s_k \in S_a$, $\Delta_k^a \geq 1$. From Corollary 1, $\forall s_k \in S_a$, it is sufficient to have $\Gamma_k = 9$ for the fault-tolerant communication connectivity within the communication region of s_k. Therefore,

$$|S_t^1| = |\bigcup_{\forall s_k \in S_a} N_k^1| \leq \sum_{\forall s_k \in S_a} |N_k^1| = \sum_{\forall s_k \in S_a} \Gamma_k \leq \sum_{\forall s_k \in S_a} 9 = 9|V_a|. \tag{13}$$

However, note that s_k can share FT nodes with its active neighbors. Assume that $s_i \in N_k^a$ and recall the six sectors in Fig. 2(a). Then s_i is connected to at least one FT node in the set N_k^1 corresponding to s_k. Let this FT node be denoted by s_j. Therefore, when s_i selects its own FT nodes, it also selects the existing FT node s_j. Since each pair of connected active nodes share at least one FT node, the total number of times that FT nodes have been shared is at least $|E_a|$. This implies that Equation (3) over-counts the size of S_t^1 by at least $|E_a|$. Therefore, $|S_t^1| \leq 9|V_a| - |E_a|$. An example is shown in Fig. 9, where $s_i \in N_k^a$ and s_j is a FT node for both s_k and s_i. ■

Proof of Theorem 4

Proof. For a Ω-DOFT ($1 < \Omega \leq \Delta_k^a$) sensor network, consider an arbitraily-chosen active node $s_k \in S_a$. To maintain connectivity over the entire sensor network, the FT nodes selected for s_k must first keep all non-failing active neighbors and sleeping neighbors connected; second, they should also provide alternative routing paths for those failing active neighbors, i.e., the network traffic going outside the communication region of s_k should not be impeded. Since s_k itself can be one of the Ω failing active nodes, the proof is based on the enumeration of the following three cases.

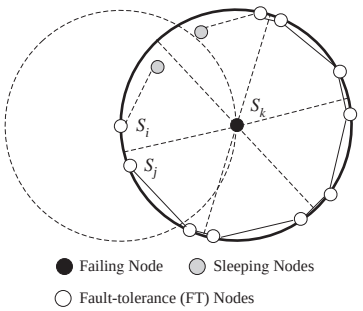


FIGURE 9 Illustration of the proof of Theorem 3.

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

Case 1: If s_k fails and $\Omega = \Delta_k^a + 1$. Since s_k fails, s_k has $\Omega - 1$ failing neighbors. Since s_k needs at most 1 FT neighbor for each failing node to provide an alternative routing path for this failing node, it is sufficient for s_k to have $\Omega - 1$ FT nodes for all failing neighbors. Furthermore, consider the connectivity within the communication region of s_k. If $\Omega = \Delta_k^a + 1$, from Theorem 1, it is sufficient to have 10 FT nodes for fault-tolerant communication connectivity within the communication region of s_k. This leads us to $\Gamma_k \geq \Omega - 1 + 10 = \Omega + 9$.

Case 2: If s_k fails and $\Omega < \Delta_k^a + 1$. Since s_k fails, similar to Case 1, it is sufficient for s_k to have $\Omega - 1$ FT nodes to provide alternative routing paths for the failing neighbors. Also because $\Omega < \Delta_k^a + 1$, there exists at least one non-failing active neighbor of s_k. From Corollary 1, it is sufficient for s_k to have 9 FT nodes for fault-tolerant communication connectivity within the communication region of s_k. Therefore, $\Gamma_k \geq \Omega - 1 + 9 = \Omega + 8$.

Case 3: If s_k does not fail. All non-failing neighbors and sleeping neighbors of s_k are still connected because s_k is active and alive. Thus we only need FT nodes to provide alternative routing paths for failing neighbors of s_k. Similar to Case 1, it is sufficient for s_k to have Ω FT nodes to provide alternative routing paths for the failing neighbors. ■

Proof of Theorem 5

Proof. Let S_f^Ω be the set of FT nodes selected when nodes in S_f fail. Consider the connectivity of corresponding subgraph G_f of S_f. There are three possible cases to consider: 1) G_f is connected. This corresponds to the case that $\forall s_i, s_j \in S_f (s_i \neq s_j)$, there is a routing path from s_i to s_j in S_f. 2) G_f is not connected and $E_f = \phi$. This means none of nodes in S_f is connected to any other nodes in S_f. 3) G_f is not connected and $E_f \neq \phi$. This corresponds to the case that $\exists s_i, s_j \in S_f (s_i \neq s_j)$ such that there is a routing path from s_i to s_j in S_f, and at the same time, $\exists s_i', s_j' \in S_f$, where $s_i \neq s_i'$ and $s_j \neq s_j'$, such that there is no routing path from s_i' to s_j' available in S_f. Let N_k^Ω be the set of nodes selected for s_k as FT nodes when s_k fails. In the following, we determine an upper bound on $|S_t^\Omega|$ for each of the three cases described earlier.

Case 1: If G_f is connected. Since nodes in G_f fail at the same time and G_f is connected, this implies that $\forall s_k \in S_f$, at least one active neighbor of s_k fails. Note that it is possible that all active neighbors of s_k fail together with s_k itself. Thus, from Theorem 1 at most 10 FT nodes are needed for s_k. Therefore,

$$|S_t^\Omega| = \Big|\bigcup_{\forall s_k \in S_a} N_k^\Omega\Big| \leq \sum_{\forall s_k \in S_a} |N_k^\Omega| \leq \sum_{\forall s_k \in S_a} 10 = 10\,|V_a|.$$

From Fig. 2(b) and Fig. 2(c), when two connected nodes fail at the same time, even the smallest overlap of their communication regions contains at least 4 FT nodes, which are FT nodes shared by both failing nodes. This implies that for each edge of $|E_a|$, there are at least 4 shared FT nodes. Therefore, from Theorem 4,

$$|S_f^\Omega| \leq 10\,|V_a| - 4\,|E_a|.$$

Case 2: If G_f is not connected and $E_f = \phi$. Obviously in this case, $\forall s_k \in S_f$, the number of FT nodes needed for s_k is the same as the number of FT nodes needed for the case

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

where $\Omega = 1$. Also, because $E_f = \phi$, $\forall s_k \in S_f$, s_k has at least one non-failing neighbor. Then from Corollary 1, at most 9 FT nodes are needed for s_k. Therefore,

$$|S_f^{\Omega}| = |\bigcup_{\forall s_k \in S_f} N_k^{\Omega}| \le \sum_{\forall s_k \in S_f} |N_k^{\Omega}| \le \sum_{\forall s_k \in S_f} 9 = 9|V_a|.$$

Case 3: If G_f is not connected and $E_f \neq \phi$. This includes non-connected failing nodes as discussed in Case 1 with no shared FT nodes and connected failing nodes as discussed in Case 2 with shared FT nodes. Since $E_f \neq \phi$, $|E_f| \ge 1$, i.e., at least two failing nodes are connected. Therefore, ■

$$|S_f^{\Omega}| \le 9(|V_a| - 2) + (10 \times 2 - 4) = 9|V_a| - 2$$

Proof of Theorem 8

Proof. Assume that $S_1 \subseteq S_i^s$ is the subset generated by the procedure in Fig. 4 as the set of FT nodes for g_i. Assume that $S_1 = L_i(1, \ldots, j, j+1)$, i.e., S_1 is obtained at the j-th position as shown by in line 8 in Fig. 4. Therefore, $q_i(L_i(1,\ldots,j,j+1)) \ge p_{th}$ and $q_i(L_i(1,\ldots,j)) < p_{th}$. Denote the node at $j+1$ in L_i as s_{k_0}, i.e, $l(s_{k_0}) = j+1$ and $L_i(j+1) = \{s_{k_0}\}$. Assume that $\exists S_2 \subseteq S_i^s$ such that $|S_2| < |S_1|$ and $q_i(S_2) \ge p_{th}$. Since both S_1 and S_2 are subsets of S_i^s, there are three cases in the relationship between S_1 and S_2, which are listed below as,

Case 1: If $S_2 \subset S_1$. Note that Since $S_1 = L_i(1,\ldots,j,j+1)$.

1. If $L_i(j+1) \not\subseteq S_2$, then $S_2 \subseteq L_i(1,\ldots,j)$. From Equation (8), $q_i(S_2) \le q_i(L_i(1,\ldots,j)) < p_{th}$, which conflicts with the assumption that $q_i(S_2) \ge p_{th}$.
2. If $L_i(j+1) \subseteq S_2$, let $S_2' = S_2 \setminus L_i(j+1)$. Since $|S_2| < |S_1|$, we have $S_2' \subset L_i(1,\cdots,j)$. Then $\exists s_{k_1} \in L_i(1,\cdots,j) \setminus S_2'$, such that $l(s_{k_1}) < l(s_{k_0})$. Based on the definition of L_i, we have $p_i^{k_0} > p_i^{k_1}$. Therefore, from Equation (8), we have

   $$q_i(S_2) = q_i(S_2' \cup L_i(j+1)) = q_i(S_2' \cup \{s_{k_0}\}) < q_i(S_2' \cup \{s_{k_1}\}) < q_i(L_i(1,\cdots,j)) < p_{th},$$

   which contradicts with the assumption that $q_i(S_2) \ge p_{th}$.

Case 2: If $S_2 \cap S_1 = \phi$. From the definition of L_i, $S_2 \subseteq L_i(j+2,\ldots,|L_i|)$. Without loss of generality, let $S_2 = L_i(u_1, u_2, \ldots, u_a)$, where $j+2 \le u_1 \le u_2 \le \ldots \le u_a \le |L_i|$. Since $|S_2| < |S_1|$, we can construct a subset S_1' of S_1, where $|S_1'| = |S_2|$ and $S_1' = L_i(v_1, v_2, \cdots, v_b)$ such that $v_1 < u_1$, $v_2 < u_2, \ldots, v_b < u_a$. Therefore, from Equation (8), $q_i(S_2) \le q_i(S_1') < p_{th}$. This contradicts with the assumption that $q_i(S_2) \ge p_{th}$.

Case 3: If $S_2 \not\subseteq S_1$ and $S_2 \cap S_1 \neq \phi$. Assume that $S_0 = S_2 \cap S_1$. Then, let $S_1' = S_1 \setminus S_0$ and $S_2' = S_2 \setminus S_0$. Obviously $S_2' \subseteq L_i(j+1,\cdots,|L_i|)$. Since $|S_1| > |S_2|$, then $|S_0| + |S_1'| > |S_0| + |S_2'| \Rightarrow |S_1'| > |S_2'|$

Downloaded By: [Zou, Yi] At: 14:01 21 July 2007

1. If $L_i(j+1) \not\subseteq S_2$, then $L_i(j+1) \not\subseteq S_0$, therefore $L_i(j+1) \subseteq S_1^{'}$. Let $S_1^{''} = S_1^{'} \setminus L_i(j+1)$. Since $|S_1^{'}| > |S_2^{'}| \Rightarrow |S_1^{''} \cup L_i(j+1)| > |S_2^{'}| \Rightarrow |S_1^{''}| \geq |S_2^{'}|$. Therefore, we can construct a subset $S_1^{*} \subseteq S_1^{''}$ such that $|S_1^{*}| = |S_2^{'}|$. Note that $S_1^{*} \subseteq L_i(1,\cdots,j)$ and $S_2^{'} \subseteq L_i(j+1,\cdots,|L_i|)$, therefore $q_i(S_1^{*}) > q_i(S_2^{'})$. Also note that $\left(S_0 \cup S_1^{*}\right) \subseteq L_i(j+1,\cdots,|L_i|)$. Thus, from Equation (8), we have

$$q_i(S_2) = q_i(S_0 \cup S_2^{'}) < q_i(S_0 \cup S_1^{*}) \leq q_i(L_i(1,\cdots,j)) < p_{th},$$

which conflicts with the assumption that $q_i(S_2) > p_{th}$.

2. If $L_i(j+1) \subseteq S_2$, then $L_i(j+1) \subseteq S_0$ because $S_2^{'} \subseteq L_i(j+1,\cdots,|L_i|)$. Let $S_0^{'} = S_0 \setminus L_i(j+1)$. Since $|S_1^{'}| > |S_2^{'}|$, we can construct a subset $S_1^{''} \subset S_1^{'}$ such that $|S_1^{''}| = |S_2^{'}|$. Further note that $S_1^{'} \setminus S_1^{''} \neq \phi$, therefore, $\exists s_{k_1} \in S_1^{'} \setminus S_1^{''}$, such that $l(s_{k_1}) < l(s_{k_0})$, i.e., $p_i^{k_1} > p_i^{k_0}$. Also note that $(S_0^{'} \cup S_1^{''} \cup \{s_{k_1}\}) \subseteq L_i(1,\cdots,j)$. Therefore, we have

$$\begin{aligned} q_i(S_2) &= q_i(S_0 \cup S_2^{'}) = q_i(S_0^{'} \cup S_2^{'} \cup L_i(j+1)) \\ &< q_i(S_0^{'} \cup S_1^{''} \cup \{s_{k_1}\}) < q_i(L_i(1,\cdots,j)) < p_{th,} \end{aligned}$$

which contradicts with the assumption that $q_i(S_2) \geq p_{th}$.

From the above discussion, for a given grid point g_i, the distributed coverage-centric selection procedure given by Fig. 4 generates the subset of FT nodes with the minimum number of FT nodes for g_i. ■